Department of Energy

Bonneville Power Administration
P.O. Box 3621
Portland, Oregon 97208-3621

FREEDOM OF INFORMATION ACT/PRIVACY PROGRAM

June 30, 2014

In reply refer to: D-B1

Mr. Kyle Iboshi
KGW
1501 SW Jefferson St
Portland, OR 97201

FOIA #BPA-2014-01197-F

Dear Mr. Iboshi:

This is a final response to your request for records under the Freedom of Information Act (5 U.S.C. § 552).

You requested:
"Copies of all security incidents reported from Bonneville Power Administration to the DOE Cyber Incident Response Capability in accordance with DOE Manual 205.1-8, Cyber Security Incident Response Manual between January 1, 2012, and June 1, 2014."

Response:
BPA found 296 incident reports (totaling 547 pages) and one summary report (9 pages) in response to your request. BPA is releasing the enclosed documents in their entirety.

There are no fees associated with this request.

Appeal:
Pursuant to Department of Energy Privacy Act regulations at 10 C.F.R. § 1008.11, you may administratively appeal this response in writing within 30 calendar days. If you choose to appeal, please include the following:

(1) A copy of your original request;
(2) A copy of the determination letter; and
(3) A statement detailing the reasons for your belief that the denial was made in error.

Clearly mark both your letter and envelope with the words "Privacy Act Appeal," and direct it to the following address:

Director, Office of Hearings and Appeals
Department of Energy
1000 Independence Avenue, SW
Washington DC 20585-1615

Should you have any questions about this letter please contact Kim Winn, FOIA Public Liaison, at 503-230-5273.

Sincerely,

/s/Christina J. Munro
Christina J. Munro
Freedom of Information/Privacy Act Officer

Enclosure: CD

	A	B	C	D	E	F	G
1	**BPA ID**	**Category**	**Sub-category**	**JC3 Ticket Number**	**Reported to CIRC**	**Report Collected for FOIA Request**	**Notes**
2		Lost	RSA SecureID Token	JC3-CIRC672456	1/4/12 0:00	Yes	
3		Lost	Standard Cell Phone	CIRC	1/4/12 0:00		Standard phones typically aren't reported.
4		Lost	RSA SecureID Token	JC3-CIR672643	1/6/12 0:00	Yes	
5		Stolen	Blackberry Smartphone	JC3-CIRC672669	1/6/12 0:00	Yes	
6		Lost	RSA SecureID Token	JC3-CIRC673181	1/13/12 0:00	Yes	
7		Lost	RSA SecureID Token	JC3-CIRC673368	1/19/12 0:00	Yes	
8		Lost	RSA SecureID Token	JC3-CIRC674717	2/13/12 0:00	Yes	Duplicate report JC3-CIRC674950
9		Lost	RSA SecureID Token	JC3-CIRC675303	2/23/12 0:00	Yes	
10		Server names posted	Server names posted external	JC3-CIRC675399	2/24/12 0:00	Yes	
11		Lost	Blackberry Smartphone	JC3-CIRC675633	2/29/12 0:00	Yes	
12		Stolen	Computer Laptop and Blackberry Smartphone	JC3-CIRC675841	3/2/12 0:00	Yes	
13		Lost	RSA SecureID Token	JC3-CIRC676031	3/6/12 0:00	Yes	
14		Lost	RSA SecureID Token	JC3-CIRC676044	3/6/12 0:00	Yes	
15		Lost	RSA SecureID Token	JC3-CIRC676073	3/6/12 0:00	Yes	
16		Lost	Blackberry Smartphone	JC3-CIRC676074	3/6/12 0:00	Yes	
17		Lost	RSA SecureID Token	JC3-CIRC676793	3/15/12 0:00	Yes	
18		Lost	RSA SecureID Token	JC3-	3/16/12 0:00		
19		Lost	RSA SecureID Token	JC3-	3/21/12 0:00	Yes	Outgoing report. Don't have copy of JC3 return.
20		Lost	RSA SecureID Token	JC3-CIRC677589	3/26/12 0:00	Yes	
21		Lost	RSA SecureID Token	JC3-CIRC677592	3/26/12 0:00	Yes	
22		Lost	RSA SecureID Token	JC3-677760	3/27/12 0:00	Yes	
23		Lost	RSA SecureID Token	JC3-678239	3/30/12 0:00	Yes	
24		Lost	Blackberry Smartphone	JC3-678241	3/30/12 0:00	Yes	
25		Lost	RSA SecureID Token	JC3-678873	4/6/12 0:00	Yes	
26		Lost	RSA SecureID Token	JC3-678896	4/6/12 0:00	Yes	
27		Lost	RSA SecureID Token	JC3-678902	4/6/12 0:00	Yes	
28		Lost	RSA SecureID Token	JC3-679094	4/10/12 0:00	Yes	
29		Lost	Blackberry Smartphone	JC3-679102	4/10/12 0:00	Yes	
30		Lost	RSA SecureID Token	JC3-679782	4/17/12 0:00	Yes	
31		Lost	RSA SecureID Token	JC3-681524	5/8/12 0:00	Yes	
32		Lost	Thumb Drive	JC3-681683	5/10/12 0:00	Yes	
33		Lost	Laptop Computer	JC3-682799	5/21/12 0:00	Yes	Laptop later found
34		Lost	RSA SecureID Token	JC3-682883	5/21/12 0:00	Yes	
35		Lost	RSA SecureID Token	JC3-682862	5/21/12 0:00	Yes	
36		Lost	RSA SecureID Token	JC3-683051	5/24/13 0:00	Yes	

	A	B	C	D	E	F	G
37		Lost	RSA SecureID Token	JC3-683205	5/29/12 0:00	Yes	
38		Lost	RSA SecureID Token	JC3-683277	5/30/12 0:00	Yes	
39		Lost	RSA SecureID Token	JC3-683274	5/30/12 0:00	Yes	
40		Lost	Laptop Computer	JC3-683450	5/31/12 0:00	Yes	
41		Lost	RSA SecureID Token	JC3-683452	5/31/12 0:00	Yes	
42		Lost	RSA SecureID Token	JC3-683540	6/1/12 0:00	Yes	
43		Lost	RSA SecureID Token	JC3-683685	6/4/12 0:00	Yes	
44		Lost	RSA SecureID Token	JC3-683912	6/6/12 0:00	Yes	
45		Lost	RSA SecureID Token	JC3-684353	6/11/12 0:00	Yes	
46		Lost	Blackberry Smartphone	JC3-684504	6/12/12 0:00	Yes	
47		Lost	Blackberry Smartphone	JC3-684679	6/13/12 0:00	Yes	
48		Lost	RSA SecureID Token	JC3-684685	6/13/12 0:00	Yes	
49		Lost	Blackberry Smartphone	JC3-685115	6/18/12 0:00	Yes	
50		Lost	RSA SecureID Token	JC3-685359	6/19/12 0:00	Yes	
51		Lost	RSA SecureID Token	JC3-685368	6/19/12 0:00	Yes	
52		Lost	RSA SecureID Token	JC3-685485	6/20/12 0:00	Yes	
53		Lost	RSA SecureID Token	JC3-685499	6/20/12 0:00	Yes	
54		Lost	RSA SecureID Token		6/21/12 0:00	Yes	May not have been logged by JC3.
55		Lost	RSA SecureID Token	JC3-685608	6/21/12 0:00	Yes	
56		Lost	RSA SecureID Token	JC3-685666	6/21/12 0:00	Yes	
57		Lost	RSA SecureID Token	JC3-685684	6/21/12 0:00	Yes	
58		Lost	Blackberry Smartphone	JC3-686006	6/26/12 0:00	Yes	
59		Lost	RSA SecureID Token	JC3-686150	6/27/12 0:00	Yes	
60		Lost	RSA SecureID Token	JC3-686341	6/29/12 0:00	Yes	
61		Lost	RSA SecureID Token	JC3-686342	6/29/12 0:00	Yes	
62		Lost	RSA SecureID Token	JC3-686708	7/5/12 0:00	Yes	
63		Lost	Blackberry Smartphone	JC3-686904	7/9/12 0:00	Yes	
64		Lost	RSA SecureID Token	JC3-687231	7/12/12 0:00	Yes	
65		Lost	Blackberry Smartphone	JC3-687243	7/12/12 17:11	Yes	
66		Lost	RSA SecureID Token	JC3-687506	7/18/12 0:00	Yes	
67		Stolen	Laptop	JC3-687662	7/19/12 12:34	Yes	
68		Stolen	Blackberry Smartphone	JC3-687661	7/19/12 12:23	Yes	
69		Lost	Blackberry Smartphone	JC3-687888	7/23/12 0:00	Yes	
70		Lost	RSA SecureID Token	JC3-687868	7/23/12 0:00	Yes	
71		Lost	RSA SecureID Token	JC3-688199	7/26/12 0:00	Yes	
72		Lost	Blackberry Smartphone	JC3-	7/30/12 0:00		
73		Lost	Blackberry Smartphone	JC3-689014	8/6/12 0:00	Yes	
74		Lost	RSA SecureID Token	JC3-689146	8/8/12 0:00	Yes	

	A	B	C	D	E	F	G
75		Lost	Laptop Computers (Two)	JC3-689644	8/16/12 0:00	Yes	
76		Lost	Blackberry Smartphone	JC3-690916	9/4/12 0:00	Yes	
77		Lost	Blackberry Smartphone	C3-691033	9/5/12 0:00	Yes	
78		Lost	RSA SecureID Token	JC3-691483	9/10/12 0:00	Yes	
79		Lost	Blackberry Smartphone	JC3-691568	9/11/12 9:09	Yes	
80		Lost	Blackberry Smartphone	JC3-692487	9/21/12 10:14	Yes	
81		Lost	RSA SecureID Token	JC3-692708	9/25/12 9:05	Yes	
82		Lost	RSA SecureID Token	JC3-692720	9/25/12 9:57	Yes	
83		Lost	RSA SecureID Token	JC3-693188	9/28/12 16:34	Yes	
84		Lost	RSA SecureID Token	JC3-693509	10/3/12 0:00	Yes	
85		Lost	RSA SecureID Token	JC3-693666	10/5/12 0:00	Yes	
86		Lost	RSA SecureID Token	JC3-693890	10/9/12 0:00	Yes	
87		Lost	Blackberry Smartphone	JC3-694452	10/15/12 0:00	Yes	
88		Lost	RSA SecureID Token	JC3-694528	10/16/12 0:00	Yes	
89		Lost	Blackberry Smartphone	JC3-694811	10/18/12 0:00	Yes	
90		Lost	Blackberry Smartphone	JC3-695072	10/22/12 0:00	Yes	
91		Lost	RSA SecureID Token	JC3-695247	10/24/12 0:00	Yes	
92		Lost	RSA SecureID Token	JC3-695275	10/24/12 0:00	Yes	
93		Lost	RSA SecureID Token	JC3-695691	10/30/12 0:00	Yes	
94		Lost	RSA SecureID Token	JC3-695763	10/31/12 0:00	Yes	
95		Stolen	RSA SecureID Token	JC3-695888	11/1/12 0:00	Yes	
96		Lost	RSA SecureID Token	JC3-696505	11/8/12 0:00	Yes	
97		Lost	RSA SecureID Token	JC3-696517	11/8/12 0:00	Yes	
98		Lost	RSA SecureID Token	JC3-696810	11/13/12 0:00	Yes	
99		Lost	RSA SecureID Token	JC3-696996	11/15/12 0:00	Yes	
100		Lost	RSA SecureID Token	JC3-697113	11/16/12 0:00	Yes	
101		Lost	RSA SecureID Token	JC3-697261	11/19/12 0:00	Yes	
102		Lost	RSA SecureID Token	JC3-697315	11/19/12 0:00	Yes	
103		Lost	RSA SecureID Token	JC3-397394	11/20/12 0:00	Yes	
104		Lost	Blackberry Smartphone	JC3-697523	11/21/12 0:00	Yes	
105		Lost	Blackberry Smartphone	JC3-697744	11/27/12 0:00	Yes	
106		Lost	Infocus and two cameras	JC3-697749	11/27/12 0:00	Yes	
107		Lost	RSA SecureID Token	JC3-698028	11/30/12 0:00	Yes	
108		Lost	Blackberry Smartphone	JC3-698601	12/6/12 0:00	Yes	
109		Lost	RSA SecureID Token	JC3-699094	12/12/12 0:00	Yes	
110		Lost	RSA SecureID Token	JC3-699882	12/21/12 0:00	Yes	
111		Lost	RSA SecureID Token	JC3-700083	12/27/12 0:00	Yes	
112		Lost	Laptop Computer	JC3-700149	12/28/12 0:00	Yes	

	A	B	C	D	E	F	G
113		Lost	RSA SecureID Token	JC3-700276	1/2/13 0:00	Yes	
114		Lost	RSA SecureID Token	JC3-700309	1/2/13 0:00	Yes	
115		Lost	Blackberry Smartphone	JC3-700392	1/3/13 0:00	Yes	
116		Lost	RSA SecureID Token	JC3-700377	1/3/13 0:00	Yes	
117		Lost	Blackberry Smartphone	JC3-700600	1/7/13 0:00	Yes	
118		Lost	Blackberry Smartphone	JC3-700845	1/9/13 0:00	Yes	
119		Lost	RSA SecureID Token	JC3-700967	1/10/13 0:00	Yes	
120		Lost	Laptop Computer	JC3-701260	1/14/13 0:00	Yes	
121		Lost	RSA SecureID Token	JC3-701998	1/22/13 0:00	Yes	
122		Lost	RSA SecureID Token	JC3-702246	1/25/13 0:00	Yes	
123		Lost	Blackberry Smartphone	JC3-702547	1/29/13 0:00	Yes	
124		Lost	Laptop Computer	JC3-702594	1/29/13 0:00	Yes	
125		Lost	RSA SecureID Token	JC3-702579	1/29/13 0:00	Yes	
126		Lost	RSA SecureID Token	JC3-702665	1/30/13 0:00	Yes	
127		Lost	RSA SecureID Token	JC3-703159	2/6/13 0:00	Yes	
128		Lost	RSA SecureID Token	JC3-703160	2/6/13 0:00	Yes	
129		Lost	RSA SecureID Token	JC3-703469	2/8/13 0:00	Yes	
130		Lost	RSA SecureID Token	JC3-703718	2/12/13 0:00	Yes	
131		Lost	RSA SecureID Token	JC3-704095	2/15/13 0:00	Yes	
132		Lost	RSA SecureID Token	JC3-704308	2/19/13 0:00	Yes	
133		Lost	RSA SecureID Token	JC3-704395	2/20/13 0:00	Yes	
134		Lost	RSA SecureID Token	JC3-704436	2/20/13 0:00	Yes	
135		Lost	Blackberry Smartphone	JC3-705523	3/7/13 0:00	Yes	
136		Lost	Laptop Computer	JC3-705518	3/7/13 0:00	Yes	
137		Lost	RSA SecureID Token	JC3-705535	3/7/13 0:00	Yes	
138		Lost	Blackberry Smartphone	JC3-705739	3/11/13 0:00	Yes	
139		Lost	Laptop Computer	JC3-705753	3/11/13 0:00	Yes	
140		Social Engineering Ph	Social Engineering Phone Call	JC3-706025	3/14/13 0:00	Yes	
141		Lost	Removable Media	JC3-706108	3/15/13 0:00	Yes	
142		Lost	RSA SecureID Token	JC3-706107	3/15/13 0:00	Yes	
143		Stolen	Blackberry Smartphone	JC3-706156	3/15/13 0:00	Yes	
144		Lost	RSA SecureID Token	JC3-706349	3/18/13 0:00	Yes	
145		Lost	RSA SecureID Token	JC3-706350	3/18/13 0:00	Yes	
146		Lost	RSA SecureID Token	JC3-706621	3/20/13 0:00	Yes	
147		Lost	RSA SecureID Token	JC3-706767	3/22/13 0:00	Yes	
148		Lost	RSA SecureID Token	JC3-706958	3/26/13 0:00	Yes	
149		Lost	RSA SecureID Token	JC3-706985	3/26/13 0:00	Yes	
150		Lost	RSA SecureID Token	JC3-707330	3/29/13 0:00	Yes	

	A	B	C	D	E	F	G
151		Stolen	Laptop Computer	JC3-707972	4/9/13 0:00	Yes	
152		Lost	RSA SecureID Token	JC3-708130	4/10/13 0:00	Yes	
153		Lost	RSA SecureID Token	JC3-708164	4/10/13 0:00	Yes	
154		PHISHING MESSAGE	PHISHING MESSAGES (INTERNAL)	JC3-708890	4/22/13 0:00	Yes	
155		Lost	RSA SecureID Token	JC3-709030	4/24/13 0:00	Yes	
156		Lost	RSA SecureID Token	JC3-709215	4/29/13 0:00	Yes	
157		Lost	RSA SecureID Token	JC3-709445	5/1/13 0:00	Yes	
158		Lost	RSA SecureID Token	JC3-709644	5/6/13 0:00	Yes	
159		Lost	RSA SecureID Token	JC3-709882	5/9/13 0:00	Yes	
160		Lost	Blackberry Smartphone	JC3-710049	5/10/13 0:00	Yes	
161		Lost	Digital Camera	JC3-710173	5/14/13 0:00	Yes	
162		Lost	Removable Media	JC3-710175	5/14/13 0:00	Yes	
163		Lost	Blackberry Smartphone	JC3-710295	5/15/13 0:00	Yes	
164		Lost	Blackberry Smartphone	JC3-710592	5/20/13 0:00	Yes	
165		Lost	RSA SecureID Token	JC3-710624	5/20/13 0:00	Yes	
166	20130603	Theft	Webmail Token		6/3/13 0:00		Have internal reports, haven't found JC3 reports
167	20130607	Lost	Webmail Token		6/7/13 0:00		Have internal reports, haven't found JC3 reports
168	20130611	Lost	Webmail Token	JC3-711884	6/11/13 0:00	Yes	
169	20130612	Lost	Webmail Token	JC3-711937	6/12/13 0:00	Yes	
170	20130620	Lost	Blackberry Smartphone	JC3-712303	6/20/13 0:00	Yes	
171	20130620	Lost	Blackberry Smartphone	JC3-712319	6/20/13 0:00	Yes	
172		Lost	RSA SecureID Token	JC3-712554	6/25/13 0:00	Yes	
173		Lost	Blackberry Smartphone	JC3-712736	6/27/13 0:00	Yes	
174		Lost	RSA SecureID Token	JC3-7129809	6/28/13 0:00	Yes	
175		Lost	RSA SecureID Token	JC3-712444	6/24/13 0:00	Yes	
176	20130701-01	Lost	Blackberry Smartphone	JC3-712847	7/1/13 0:00	Yes	
177	20130702-01	Lost	RSA SecureID Token	JC3-712303	7/2/13 0:00	Yes	Note that form and body of message from JC3 say 712303, Subject says 712930, which seems to fit with one later in day that was numbered 712948.
178	20130702-02	Lost	Blackberry Smartphone	JC3-712948	7/2/13 0:00	Yes	
179	20130708-01	Lost	RSA SecureID Token	JC3-713180	7/8/13 6:49	Yes	
180	20130709-01	Lost	RSA SecureID Token	JC3-713277	7/9/13 11:22	Yes	
181	20130711-01	Lost	RSA SecureID Token	JC3-713499	7/11/13 16:19	Yes	
182	20130716-01	Lost	Laptop	JC3-713692	7/16/13 13:16	Yes	
183	20130716-02	Lost	RSA SecureID Token	JC3-713693	7/16/13 13:31	Yes	

	A	B	C	D	E	F	G
184	20130716-03	Lost	RSA SecureID Token	JC3-713713	7/16/13 16:09	Yes	
185	20130717-02	Lost	Blackberry Smartphone	JC3-713803	7/17/13 17:30	Yes	
186	20130731-02	Lost	RSA SecureID Token	JC3-714526	7/31/13 17:11	Yes	
187	20130801-01	Lost	Blackberry Smartphone	JC3-714562	8/1/13 8:53	Yes	
188	20130802-01	Lost	RSA SecureID Token	JC3-714645	8/2/13 12:26	Yes	
189	20130807-02	Lost	RSA SecureID Token	JC3-714874	8/7/13 12:25	Yes	
190	20130812-01	Lost	Blackberry Smartphone	JC3-715182	8/12/13 10:08	Yes	
191	20130821-01	Lost	Blackberry Smartphone	JC3-715821	8/21/13 15:57	Yes	
192	20130827-01	Lost	RSA SecureID Token	JC3-716184	8/27/13 14:21	Yes	
193	20130828-01	Lost	RSA SecureID Token	JC3-716261	8/28/13 10:09	Yes	
194	20130829-01	Lost	Blackberry Smartphone	JC3-716316	8/29/13 8:52	Yes	
195	20130829-02	Lost	RSA SecureID Token	JC3-716325	8/29/13 9:38	Yes	
196	20130830-02	Lost	Blackberry Smartphone	JC3-716420	8/30/13 14:23	Yes	
197	20130903-01	Lost	Laptop	JC3-716463	9/3/13 11:09	Yes	
198	20130903-02	Lost	Laptop	JC3-716470	9/3/13 13:22	Yes	
199	20130909-01	Lost	RSA SecureID Token	JC3-716778	9/9/13 11:29	Yes	
200	20130911-01	Lost	Blackberry Smartphone	JC3-716976	9/11/13 14:41	Yes	
201	20130916-01	Lost	RSA SecureID Token	JC3-717200	9/16/13 15:57	Yes	
202	20130916-02	Lost	RSA SecureID Token	JC3-717201	9/16/13 16:39	Yes	
203	20130917-01	Lost	RSA SecureID Token	JC3-717229	9/17/13 9:55	Yes	
204	20130917-02	Lost	Blackberry Smartphone	JC3-717233	9/17/13 10:19	Yes	
205	20130924-01	Lost	Removable Media	JC3-717597	9/24/13 10:04	Yes	
206	20131001-02	Lost	RSA SecureID Token	JC3-718059	10/1/13 15:10	Yes	
207	20131002-01	Lost	Blackberry Smartphone	JC3-718093	10/2/13 11:48	Yes	
208	20131003-01	Lost	RSA SecureID Token	JC3-718200	10/3/13 13:04	Yes	
209	20131007-02	Lost	Blackberry Smartphone	JC3-718377	10/7/13 12:49	Yes	
210	20131008-02	Lost	RSA SecureID Token	JC3-718400	10/8/13 8:32	Yes	
211	20131008-01	Lost	RSA SecureID Token	JC3-718430	10/8/13 13:29	Yes	
212	20131009-02	Lost	RSA SecureID Token	JC3-718549	10/9/13 16:18	Yes	
213	20131009-01	Lost	RSA SecureID Token	JC3-718563	10/9/13 17:58	Yes	
214	20131016-01	Lost	RSA SecureID Token	JC3-718830	10/16/13 14:07	Yes	
215	20131016-02	Lost	RSA SecureID Token	JC3-718843	10/16/13 16:11	Yes	
216	20131017-01	Lost	Blackberry Smartphone	JC3-718913	10/17/13 13:13	Yes	
217	20131018-01	Theft	Laptop	JC3-718966	10/18/13 6:42	Yes	
218	20131018-02	Lost	RSA SecureID Token	JC3-718978	10/18/13 7:44	Yes	
219	20131021-02	Lost	RSA SecureID Token	JC3-719109	10/21/13 15:43	Yes	
220	20131022-02	Lost	Blackberry Smartphone	JC3-719163	10/22/13 10:30	Yes	
221	20131024-02	Lost	RSA SecureID Token	JC3-719354	10/24/13 14:49	Yes	

	A	B	C	D	E	F	G
222	20131025-01	Lost	RSA SecureID Token	JC3-719408	10/25/13 10:38	Yes	
223	20131028-01	Lost	RSA SecureID Token	JC3-719528	10/28/13 11:05	Yes	
224	20131029-01	Lost	Blackberry Smartphone	JC3-719610	10/29/13 15:07	Yes	
225	20131106-01	Lost	Help Desk	JC3-719958	11/6/13 10:04	Yes	
226	20131113-01	Lost	RSA SecureID Token	JC3-720305	11/13/13 10:10	Yes	
227	20131113-02	Lost	RSA SecureID Token	JC3-720334	11/13/13 17:57	Yes	
228	20131114-01	Lost	RSA SecureID Token	JC3-720366	11/14/13 10:27	Yes	
229	20131120-01	Lost	Blackberry Smartphone	JC3-720693	11/20/13 16:06	Yes	
230	20131121-01	Lost	Blackberry Smartphone	JC3-720760	11/21/13 14:35	Yes	
231	20131122-01	Lost	Blackberry Smartphone	JC3-720806	11/22/13 11:12	Yes	
232	20131125-02	Lost	Blackberry Smartphone	JC3-720907	11/25/13 12:40	Yes	
233	20131203-03	Lost	RSA SecureID Token	JC3-721150	12/3/13 9:49	Yes	
234	20131203-02	Information Compromise		JC3-721171	12/3/13 16:15	Yes	
235	20131204-01	Lost	Blackberry Smartphone	JC3-721269	12/4/13 15:27	Yes	
236	20131209-01	Lost	Blackberry Smartphone	JC3-721521	12/9/13 14:14	Yes	
237	20131211-01	Lost	RSA SecureID Token	JC3-721602	12/11/13 9:05	Yes	
238	20131211-02	Lost	Laptop	JC3-721603	12/11/13 9:05	Yes	
239	20131217-01	Lost	Blackberry Smartphone	JC3-721824	12/17/13 10:30	Yes	
240	20131217-02	Lost	Laptop	JC3-721836	12/17/13 12:25	Yes	
241	20131219-03	Lost	RSA SecureID Token	JC3-721951	12/19/13 14:11	Yes	
242	20131223-01	Unauthorized Use	Web Site Defacement	JC3-722083	12/23/13 0:00	Yes	
243	20131224-01	Unauthorized Use	Web Site Defacement	JC3-722093	12/24/13 0:00	Same incident as JC3-722093	
244	20131231-01	Lost	RSA SecureID Token	JC3-722318	12/31/13 10:32	Yes	
245	20131231-02	Lost	Blackberry Smartphone	JC3-722324	12/31/13 11:58	Yes	
246	20140103-01	Lost	RSA SecureID Token	JC3-722415	1/3/14 9:09	Yes	
247	20140106-01	Lost	RSA SecureID Token	JC3-722553	1/6/14 15:11	Yes	
248	20140108-01	Lost	Blackberry Smartphone	JC3-722654	1/8/14 8:24	Yes	
249	20140108-03	Lost	RSA SecureID Token	JC3-722678	1/8/14 12:28	Yes	
250	20140114-01	Lost	RSA SecureID Token	JC3-722915	1/14/14 8:56	Yes	
251	20140114-02	Lost	Laptop	JC3-722973	1/14/14 14:16	Yes	
252	20140127-01	Lost	Blackberry Smartphone	JC3-723586	1/27/14 7:11	Yes	
253	20140128-01	Lost	Blackberry Smartphone	JC3-723673	1/28/14 13:30	Yes	
254	20140204-02	Lost	Laptop Computer	JC3-723999	2/4/14 17:00	Yes	
255	20140206-01	Lost	RSA SecureID Token	JC3-724070	2/6/14 7:39	Yes	
256	20140210-01	Lost	RSA SecureID Token	JC3-724230	2/10/14 14:08	Yes	
257	20140210-02	Lost	Blackberry Smartphone	JC3-724240	2/10/14 15:05	Yes	
258	20140211-01	Lost	Blackberry Smartphone	JC3-724303	2/11/14 16:57	Yes	
259	20140212-01	Lost	Laptop Computer	JC3-724346	2/12/14 9:44	Yes	

	A	B	C	D	E	F	G
260	20140218-02	Lost	Blackberry Smartphone	JC3-724655	2/18/14 7:36	Yes	
261	20140218-03	Lost	RSA SecureID Token	JC3-724665	2/18/14 9:19	Yes	
262	20140219-01	Lost	RSA SecureID Token	JC3-724738	2/19/14 8:28	Yes	
263	20140220-01	Lost	RSA SecureID Token	JC3-724903	2/20/14 17:07	Yes	
264	20140221-02	Lost	RSA SecureID Token	JC3-724952	2/21/14 0:00	Yes	
265	20140224-01	Lost	RSA SecureID Token	JC3-725094	2/24/14 11:16	Yes	
266	20140226-01	Lost	Laptop	JC3-725238	2/26/14 12:29	Yes	
267	20140303-01	Lost	RSA SecureID Token	JC3-725429	3/3/14 7:43	Yes	
268	20140306-01	Lost	RSA SecureID Token	JC3-725581	3/6/14 8:35	Yes	
269	20140306-02	Lost	Blackberry Smartphone	JC3-725588	3/6/14 9:00	Yes	
270	20140313-01	Lost	Blackberry Smartphone	JC3-725877	3/13/14 9:23	Yes	
271	20140319-01	Lost	RSA SecureID Token	JC3-726157	3/19/14 9:25	Yes	
272	20140321-01	Lost	RSA SecureID Token	JC3-726297	3/21/14 11:21	Yes	
273	20140402-02	Lost	Laptops	JC3-726976	4/2/14 0:00	Yes	
274	20140402-01	Lost	RSA SecureID Token	JC3-726768	4/2/14 12:53	Yes	
275	20140403-02	Lost	Blackberry Smartphone	JC3-727015	4/3/14 14:32	Yes	
276	20140404-01	Lost	RSA SecureID Token	JC3-727093	4/4/14 15:00	Yes	
277	20140410-01	Lost	Blackberry Smartphone	JC3-727371	4/10/14 8:11	Yes	
278	20140411-01	Lost	Blackberry Smartphone	JC3-727450	4/11/14 9:13	Yes	
279	20140414-01	Lost	RSA SecureID Token	JC3-727556 (CIRC Originally listed it as 727555)	4/14/14 11:22	Yes	
280	20140414-02	Lost	Blackberry Smartphone	JC3- 727583	4/14/14 14:03	Yes	
281	20140415-01	Lost	Blackberry Smartphone	JC3-727647	4/15/14 8:54	Yes	
282	20140417-01	Lost	RSA SecureID Token	JC3-727864	4/17/14 13:59	Yes	
283	20140418-01	Lost	Blackberry Smartphone	JC3-727907	4/18/14 8:18	Yes	
284	20140421-01	Lost	Blackberry Smartphone	JC3-728098	4/21/14 9:56	Yes	
285	20140423-01	Lost	RSA SecureID Token	JC3-728265	4/23/14 11:45	Yes	
286	20140428-03	Lost	RSA SecureID Token	JC3-728552	4/28/14 15:28	Yes	
287	20140429-01	Lost	Blackberry Smartphone	JC3-728622	4/29/14 0:00	Yes	
288	20140501-02	Lost	RSA SecureID Token	JC3-728895	5/1/14 0:00	Yes	
289	20140501-01	Lost	Blackberry Smartphone	JC3-728887	5/1/14 13:15	Yes	
290	20140502-01	Lost	RSA SecureID Token	JC3-728943	5/2/14 12:26	Yes	
291	20140505-01	Lost	Laptop Computer	JC3-729035	5/5/14 10:07	Yes	
292	20140505-02	Lost	Blackberry Smartphone	JC3-729057	5/5/14 13:47	Yes	
293	20140506-01	Lost	Laptop Computer	JC3-729103	5/6/14 8:07	Yes	
294	20140506-02	Lost	Blackberry Smartphone	JC3-729147	5/6/14 13:05	Yes	
295	20140506-03	Lost	Desktop Computer	JC3-729164	5/6/14 14:51	Yes	

	A	B	C	D	E	F	G
296	20140514-01	Lost	Blackberry Smartphone	JC3-729589	5/14/14 16:01	Yes	
297	20140515-01	Lost	Blackberry Smartphone	JC3-729620	5/15/14 9:22	Yes	
298	20140520-01	Lost	RSA SecureID Token	JC3-729858	5/20/14 8:31	Yes	
299	20140520-02	Lost	RSA SecureID Token	JC3-729877	5/20/14 10:55	Yes	
300	20140521-01	Lost	Blackberry Smartphone	JC3- 729933	5/21/14 13:39	Yes	
301	20140522-01	Lost	RSA SecureID Token	JC3-730066	5/22/14 15:51	Yes	
302	20140530-01	Lost	Blackberry Smartphone	JC3-730396	5/30/14 0:00	Yes	
303	20140530-03	Information Comprom	SSN List	JC3-730430	5/30/14 15:38	Yes	
304							

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 717201** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 09/16/13
Time incident *occurred*:	**Time incident *discovered*:** 4:35pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 09/16/13 at approximately 4:35pm PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 9/16/2013	**Report Time:7:39 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 724303** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02-11-2014
Time incident *occurred*:	**Time incident *discovered*:** 4:50 pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:2/11/2014	**Report Time:9:28 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 728622** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: CBS Support Desk – Anthony Weissman	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4161	**Email address:** cbssupportdesk@bpa.gov
Incident Information	
Date incident *occurred*: 4/26/14	**Date incident *discovered*:** 4/29/14
Time incident *occurred*:	**Time incident *discovered*:** 0826

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Yes Was the drive(s) or file(s) password protected? Yes Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category – Low

The BPA Blackberry was discovered lost on 4/26/14, the user discovered that someone found his phone by calling it and the person who found the Blackberry agreed to meet to return the phone. The phone was returned to the user on 4/28/14 at 6:00 p.m. Upon return the user realized the Blackberry had been wiped clean. The user doesn't know where or at what time the device was lost and picked up by someone.

On 04/29/14 at approximately 8:26 a.m. PST, the BPA CBS Support Desk received a report of a missing/lost blackberry smart phone.

There was no known PII or SUI information on the device. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated if further information becomes available.

Method of detection:
Phone call

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken: Smartphone has been wiped clean.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify) **BPA Cyber Security**	
Report Information (Call Center Use Only)	
Report Date: 4/29/2014	**Report Time: 12:03 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #:** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** March 21, 2012
Time incident *occurred*:	**Time incident *discovered*:** 10:30 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On March 21, 2012 at approximately 10:30 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:	**Report Time:**

U.S. Department of Energy
Office of the Chief Information Officer
Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report

Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 675303** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: Gary Prouse	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-3667	**Email address:** glprouse@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** February 23, 2012
Time incident *occurred*:	**Time incident *discovered*:** 08:01 a.m. PST

Type 1 Incident:

System Compromise/Intrusion
- ☐ Root Compromise ☐ User Compromise

Loss, Theft, or Missing
- ☐ Desktop ☐ Laptop ☐ Media ☒ Other (webmail token)

Malicious Code
- ☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)

☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:

☐ IP - ☐ PF - ☐ PS - ☐ PPM -

IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
On February 23, 2012 at 08:01 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.
We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 2/23/2012	**Report Time: 4:01 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: JC3-677760** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** March 27, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:20 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On March 27, 2012 at 11:20 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/27/2012	**Report Time: 3:00 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 678239** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** March 30, 2012
Time incident *occurred*:	**Time incident *discovered*:** 10:25 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA SecurID webmail token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
On March 30, 2012 at 10:25 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.
We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 3/30/2012	**Report Time: 2:07 pm ET**

OFFICIAL USE ONLY

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 678241** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** March 30, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:00 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Blackberry)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
On March 30, 2012 at approximately 11:00 a.m. PST, the Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.There was no known PII or SUI information on the device.This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Phone service has been terminated.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 3/30/2012	**Report Time: 2:44 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 678873** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** April 6, 2012
Time incident *occurred*:	**Time incident *discovered*:** 10:00 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
On April 6, 2012 at 10:00 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 4/6/2012	Report Time: 1:30 pm ET

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 678896** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** April 6, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:10 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA SecurID webmail token.)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
On April 6, 2012 at 11:10 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.
We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:
Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken
Assessment of the impact of the incident:
What actions have been taken:
RSA Webmail Token has been disabled

Other Information
Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 4/6/2012	**Report Time: 2:42 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 678902** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** April 6, 2012
Time incident *occurred*:	**Time incident *discovered*:** 12:20 p.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA webtoken)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
On April 6, 2012 at 12:20 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 4/6/2012	Report Time: 3:47 pm ET

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 679094** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** April 10, 2012
Time incident *occurred*:	**Time incident *discovered*:** 10:16 a.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: 1	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On April 10, 2012 at approximately 10:16 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken: Token has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	

Report Information (Call Center Use Only)	
Report Date: 4/10/2012	Report Time: 2:11 pm ET

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 679102** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** April 10, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:22 a.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Blackberry)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On April 10, 2012 at approximately 11:22 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated. There was no known PII or SUI information on the device. This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Blackberry device has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/10/2012	**Report Time: 3:23 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 679782** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** April 17, 2012
Time incident *occurred*:	**Time incident *discovered*:** 5:15 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On April 17, 2012 at approximately 5:15 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: RSA token has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/17/2012	**Report Time: 8:31 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 681524** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: 5/8/2012	**Date incident *discovered*:** 5/8/2012
Time incident *occurred*:	**Time incident *discovered*:** 9:45 a.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On May 8, 2012 at approximately 9:45 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: RSA token has been disabled.

Other Information

Who has been notified?

☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/8//2012	**Report Time: 1:35 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 681683** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: 5/10/2012	**Date incident *discovered*:** 5/10/2012
Time incident *occurred*:	**Time incident *discovered*:** 3:55 PM ET

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On May 10, 2012 at 12:10 p.m. PST, the BPA Office of Cyber Security received a report of a lost thumb drive (Government owned removable media)

There was no PII or SUI information on the thumb drive.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information

Who has been notified?

☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/10//2012	**Report Time: 3:55 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 682799** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: 5/21/2012	**Date incident *discovered*:** 5/21/2012
Time incident *occurred*: 10:15 AM PT	**Time incident *discovered*:** 10:15 AM PT

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On May 21, 2012 at 10:15 a.m. PST, the BPA Office of Cyber Security received a report of a lost laptop computer.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec. The VPN certificate allowing remote access has been revoked.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information

Who has been notified?

☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/21//2012	**Report Time: 1:21 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 682862** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: 5/21/2012	**Date incident *discovered*:** 5/21/2012
Time incident *occurred*: 1:40 PM PT	**Time incident *discovered*:** 1:40 PM PT

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On May 21, 2012 at approximately 1:40 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/21//2012	**Report Time: 5:12 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 682883** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: 5/21/2012	**Date incident *discovered*:** 5/21/2012
Time incident *occurred*: 4:10 PM PT	**Time incident *discovered*:** 4:10 PM PT

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On May 21, 2012 at approximately 4:10 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information

Who has been notified?

☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/21//2012	**Report Time: 7:36 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 683051** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: 5/24/2012	**Date incident *discovered*:** 5/24/2012
Time incident *occurred*: 1:45 PM PT	**Time incident *discovered*:** 1:45 PM PT

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On May 24, 2012 at approximately 1:45 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/24//2012	**Report Time: 5:22 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 683205 (CLOSED)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*: 5/29/2012	**Date incident *discovered*:** 5/29/2012
Time incident *occurred*: 12:50 PM PT	**Time incident *discovered*:** 12:50PM PT

Type 1 Incident:

System Compromise/Intrusion
- ☐ Root Compromise ☐ User Compromise

Loss, Theft, or Missing
- ☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA Token)

Malicious Code
- ☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)

☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -

IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On May 29, 2012 at approximately 12:50 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 5/29/2012	**Report Time: 4:41 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 683274 (closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: May 30, 2012	**Date incident *discovered*:** May 30, 2012
Time incident *occurred*:	**Time incident *discovered*:** 12:35 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On May 30, 2012 at approximately 12:35 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:05/30/2012	**Report Time: 4:12 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #:** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** May 30, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:45 a.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On May 30, 2012 at approximately 11:45 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:	**Report Time:**

From: JC3 <circ@jc3.doe.gov>
Sent: Thursday, May 31, 2012 8:01 PM
To: McCann,April A (BPA) - NJB-B1
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry,Sean P (BPA) - NJB-B1; JC3
Subject: JC3-683450 : INCIDENT REPORT - Lost Laptop Computer

To Whom It May Concern,

This information was reported to JC3 on 5/31/2012 at 9:47 pm ET. The JC3 has assigned ticket number JC3-683450 to this Incident. Please reference this ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

Minkah Ali
U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3 Call Center
1-866-941-2472
circ@jc3.doe.gov

From: McCann,April A (BPA) - NJB-B1 [mailto:aamccann@bpa.gov]
Sent: Thursday, May 31, 2012 9:47 PM
To: JC3
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry, Sean
Subject: INCIDENT REPORT - Lost Laptop Computer

Type 1 Incident / Security Category - Low
On May 31, 2012 at 6:35 p.m. PST, the BPA Office of Cyber Security received a report of a lost laptop computer.
There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.
This case will be updated as further information becomes available.
April A. D. McCann, NJB-B1
IT Specialist, Cyber Security
Bonneville Power Administration (BPA) - U.S. DOE
503.230-5467 / aamccann@bpa.gov
Cyber Security Main number - 503.230-5200
Cyber Security Emergency number - 503.230-5088

From: JC3 <circ@jc3.doe.gov>
Sent: Thursday, May 31, 2012 8:20 PM
To: McCann,April A (BPA) - NJB-B1
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry,Sean P (BPA) - NJB-B1; JC3
Subject: JC3-683452 : INCIDENT REPORT - Missing/Lost RSA SecurID Webmail Token

To Whom It May Concern,

This information was reported to JC3 on 5/31/2012 at 9:50 pm ET. The JC3 has assigned ticket number JC3-683452 to this Incident. Please reference this ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

Minkah Ali

U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3 Call Center
1-866-941-2472
circ@jc3.doe.gov

From: McCann,April A (BPA) - NJB-B1 [mailto:aamccann@bpa.gov]
Sent: Thursday, May 31, 2012 9:50 PM
To: JC3
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry, Sean
Subject: INCIDENT REPORT - Missing/Lost RSA SecurID Webmail Token

Type 1 Incident / Security Category - Low

On May 31, 2012 at approximately 6:40 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

April McCann

April A. D. McCann, NJB-B1
IT Specialist, Cyber Security
Bonneville Power Administration (BPA) - U.S. DOE
503.230-5467 / aamccann@bpa.gov
Cyber Security Main number - 503.230-5200
Cyber Security Emergency number - 503.230-5088

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 683540 (closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*: June1, 2012	**Date incident *discovered*:** June1, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:40 a.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category – Low** On June 1, 2012 at approximately 11:40 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/1/2012	**Report Time: 3:28 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: BPA	**For Call Center use only:** **JC3 Ticket #: 683685 (Closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503.230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*: June 4, 2012	**Date incident *discovered*:** June 4, 2012
Time incident *occurred*: 12:15 p.m. PST	**Time incident *discovered*:** 12:15 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Web Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: N/A	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: On June 4, 2012 at approximately 12:15 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date:06/04/2012	**Report Time: 4:06PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: BPA	**For Call Center use only:** **JC3 Ticket #: 683912 (Open/Closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503.230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*: June 6, 2012	**Date incident *discovered*:** June 6, 2012
Time incident *occurred*: 2:15 p.m. PST	**Time incident *discovered*:** 2:15 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (webmail token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: N/A	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: On June 6, 2012 at approximately 2:15 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: The appropriate staff has been notified and the webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/6/2012	**Report Time: 6:12 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 684353 (Closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*: June 11, 2012	**Date incident *discovered*:** June 11, 2012
Time incident *occurred*: 12:45 p.m. PST	**Time incident *discovered*:** 12:45 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Web Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: On June 11, 2012 at approximately 12:45 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: Mon 6/11/2012	**Report Time: 4:42 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 684504** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** June 12, 2012
Time incident *occurred*:	**Time incident *discovered*:** 10:30 a.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (blackberry)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On June 12, 2012 at approximately 10:30 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.

There was no known PII or SUI information on the device.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Blackberry device has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 6/12/2012	**Report Time: 2:26 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 684679** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** June 13, 2012
Time incident *occurred*:	**Time incident *discovered*:** 1:55 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Blackberry)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category - Low**
On June 13, 2012 at approximately 1:55 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated. There was no known PII or SUI information on the device. This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Blackberry device has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date:06/13/2012	**Report Time:5:44 Pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 684685 (Closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** June 13, 2012
Time incident *occurred*:	**Time incident *discovered*:** 1:50 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Webmail Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: N/A	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category - Low**
On June 13, 2012 at approximately 1:50 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/13/2012	**Report Time: 5:27 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 685115** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** June 18, 2012
Time incident *occurred*:	**Time incident *discovered*:** 12:15 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Blackberry)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category - Low**
On June 18, 2012 at approximately 12:15 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.There was no known PII or SUI information on the device.This case will be updated as further information becomes available.

Method of detection: Cyber Security received a report of a missing/lost Blackberry smartphone

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Blackberry device has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 6/18/2012	**Report Time: 4:04 Pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 685359** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** June 19, 2012
Time incident *occurred*:	**Time incident *discovered*:** 4:10 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (webmail token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category - Low**
On June 19, 2012 at approximately 4:10 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/19/2012	**Report Time: 7:30 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 685368** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** June 19, 2012
Time incident *occurred*:	**Time incident *discovered*:** 5:25 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (webmail token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:Type 1 Incident / Security Category - Low
On June 19, 2012 at approximately 5:25 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/19/2012	**Report Time: 8:49 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 685485** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** June 20, 2012
Time incident *occurred*:	**Time incident *discovered*:** 1:55 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:Type 1 Incident / Security Category - Low
On June 20, 2012 at approximately 1:55 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/20/2012	**Report Time: 5:37 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 685499** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** June 20, 2012
Time incident *occurred*:	**Time incident *discovered*:** 3:00 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category - Low**
On June 20, 2012 at approximately 3:00 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/20/2012	**Report Time: 6:38 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 685608** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** June 21, 2012
Time incident *occurred*:	**Time incident *discovered*:** 12:05 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:Type 1 Incident / Security Category - Low
On June 20, 2012 at approximately 12:05 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 6/21/2012	**Report Time: 3:41 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 685666** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** June 21, 2012
Time incident *occurred*:	**Time incident *discovered*:** 1:20 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category – Low** On June 20, 2012 at approximately 1:20 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/21/2012	**Report Time: 5:14 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 685684** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** June 21, 2012
Time incident *occurred*:	**Time incident *discovered*:** 4:25 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category – Low** On June 20, 2012 at approximately 4:25 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/21/2012	**Report Time: 8:18 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 686006** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: Gary Prouse	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-3667	**Email address:** glprouse@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** June 26, 2012
Time incident *occurred*:	**Time incident *discovered*:** 07:30 a.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Blackberry)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: 1	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category – Low** On June 26, 2012 at approximately 7:30 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated. There was no known PII or SUI information on the device. This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Blackberry device has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/26/2012	**Report Time: 2:57 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 686150** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** June 27, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:15 a.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On June 27, 2012 at approximately 11:15 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 6/27/2012	**Report Time: 2:59 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 686341 (Closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** June 29, 2012
Time incident *occurred*:	**Time incident *discovered*:** 2:15 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (TOKEN)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category – Low** On June 29, 2012 at approximately 2:15 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 6/29/2012	**Report Time: 6:01 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 686342 (Closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** June 29, 2012
Time incident *occurred*:	**Time incident *discovered*:** 3:00 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Webmail Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category – Low** On June 29, 2012 at approximately 3:00 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 6/29/2012	**Report Time: 6:40 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 686708** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** July 5, 2012
Time incident *occurred*:	**Time incident *discovered*:** 10:35 a.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On July 5, 2012 at approximately 10:35 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 7/5/2012	**Report Time: 1:56 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 686904** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** July 9, 2012
Time incident *occurred*:	**Time incident *discovered*:** 10:15 a.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On July 9, 2012 at approximately 10:15 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.

There was no known PII or SUI information on the device.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Blackberry device has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 7/9/2012	**Report Time: 1:59 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 687231** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** July 12, 2012
Time incident *occurred*:	**Time incident *discovered*:** 3:10 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category - Low**
On July 12, 2012 at approximately 3:10 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.
We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 7/12/2012	**Report Time: 6:25 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #:** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** July 12, 2012
Time incident *occurred*:	**Time incident *discovered*:** 4:40 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On July 12, 2012 at approximately 4:40 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.

There was no known PII or SUI information on the device.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Blackberry device has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:	**Report Time:**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 687506** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** July 18, 2012
Time incident *occurred*:	**Time incident *discovered*:** 7:15 a.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On July 18, 2012 at approximately 7:15 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 7/18/2012	**Report Time: 10:59 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 687661** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** July 19, 2012
Time incident *occurred*:	**Time incident *discovered*:** 12:05 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Blackberry)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On July 19, 2012 at approximately 12:05 p.m. PST, the BPA Office of Cyber Security received a report of a stolen Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.
There was no known PII or SUI information on the device.
This case will be updated as further information becomes available.

Method of detection: Office of Cyber Security received a report

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Blackberry device has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 7/19/2012 3:23 PM	**Report Time: 3:23 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 687662** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** July 19, 2012
Time incident *occurred*:	**Time incident *discovered*:** 12:05 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
Type 1 Incident / Security Category - Low

On July 19, 2012 at 12:05 p.m. PST, the BPA Office of Cyber Security received a report of a stolen laptop computer. There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec. The VPN certificate allowing remote access has been revoked. This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:
Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken
Assessment of the impact of the incident:
What actions have been taken:
Remote Access has been disabled.

Other Information
Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 7/19/2012	**Report Time: 3:34 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 687868** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** July 23, 2012
Time incident *occurred*:	**Time incident *discovered*:** 10:00 a.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On July 23, 2012 at approximately 10:00 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 7/23/2012	**Report Time: 1:48 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 687888** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** July 23, 2012
Time incident *occurred*:	**Time incident *discovered*:** 1:15 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On July 23, 2012 at approximately 1:15 p.m. PST, the BPA Office of Cyber Security received a report of a stolen Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.
There was no known PII or SUI information on the device.
This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Blackberry device has been disabled.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 7/23/2012	**Report Time: 4:47 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 688199** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: 7/26/2012	**Date incident *discovered*:** 7/26/2012
Time incident *occurred*: 12:05 p.m. PST	**Time incident *discovered*:** 7/26/2012

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On July 26, 2012 at approximately 12:05 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 7/26//2012	**Report Time: 3:35 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 689014** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: 8/6/2012	**Date incident *discovered*:**
Time incident *occurred*: 5:30 p.m. PST	**Time incident *discovered*:**

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Blackberry))
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On August 6, 2012 at approximately 5:30 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.

There was no known PII or SUI information on the device.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/6/2012	**Report Time: 9:06 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #:** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** August 8, 2012
Time incident *occurred*:	**Time incident *discovered*:** 12:50 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On August 8, 2012 at approximately 12:50 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:	**Report Time:**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 689644** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: 8/16/2012	**Date incident *discovered*:**
Time incident *occurred*: 3:15 p.m. PST	**Time incident *discovered*:**

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (2 Laptops)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On August 16, 2012 at approximately 3:15 p.m. PST, the BPA Office of Cyber Security received a report of two missing/lost laptop computers. The computers were noted missing when custodians were conducting a routine inventory check.

There was no known PII or SUI information on the computers PointSec encryption software was installed on both computers. The VPN certificate allowing remote access has been revoked.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken:	

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/16/2012	**Report Time: 6:56 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 692487** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 9/20/2012	**Date incident *discovered*:**
Time incident *occurred*: 12:00 PST	**Time incident *discovered*:**

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [09/20/2012] at approximately [12:00] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken:	

Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 9/21/2012	**Report Time: 1:15 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 692708** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 9/25/12
Time incident *occurred*:	**Time incident *discovered*:** 8:17 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category - Low**

On 09/25/12 at approximately 8:17 AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 9/25/2012	**Report Time: 12:05 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 692720** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 09-25-12
Time incident *occurred*:	**Time incident *discovered*:** 0950hrs

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category - Low**

On 09-25-12 at approximately 0950 hrs PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 9/25/2012 12:57 PM	**Report Time: 12:57 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 693188** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 9/28/2012	**Report Time: 7:34 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 693509** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 10/3/2012	**Date incident *discovered*:** 10/3/2012
Time incident *occurred*: 2:00pm	**Time incident *discovered*:** 3:42 pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On 10/3/2012 at approximately 2:00pm PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/3/2012	**Report Time: 7:05 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 693666** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/05/2012
Time incident *occurred*:	**Time incident *discovered*:** 9:00 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On 10/5/12 at approximately 9:00am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Webmail token has been disabled	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/05/2012	**Report Time: 12:10 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 693890** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/09/2012
Time incident *occurred*:	**Time incident *discovered*:** 2:14pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 10/9/2012	**Report Time: 6:00 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #:** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in date Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in time Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:	**Report Time:**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 694528** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/16/2012
Time incident *occurred*:	**Time incident *discovered*:** 8:20am PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other RSA Token
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/16/2012 at approximately 8:21am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken: Webmail token has been disabled	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/16/2012	**Report Time: 12:29 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 694811** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/18/2012
Time incident *occurred*:	**Time incident *discovered*:** 4:15pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On 10/18/2012 4:15 PM PT the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/18/2012	**Report Time: 7:58 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 695072** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: October 19, 2012	**Date incident *discovered*:** October 21, 2012
Time incident *occurred*: 9:00 pm. – 10:30 p.m.	**Time incident *discovered*:** 9:00 AM PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On October 21, 2012 at approximately 9:00 AM PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/22/2012	**Report Time: 12:13 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 695247** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 10/23/12	**Date incident *discovered*:** [10/24/12]
Time incident *occurred*: 5:00pm	**Time incident *discovered*:** [7:30 am]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -

IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/24/12 at approximately 7:30am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/24/2012	**Report Time: 10:45 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 695275** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: Approx. 1 Year Ago	**Date incident *discovered*:** [10/23/12 2:40pm]
Time incident *occurred*: Unknown	**Time incident *discovered*:** [10/23/12 2:40pm]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/24/2012	**Report Time: 1:13 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 695691** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [10-30-2012]
Time incident *occurred*:	**Time incident *discovered*:** [1:08 PM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [10-30-2012] at approximately [1:08 PM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/30/2012	**Report Time: 4:53 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 695763** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/31/2012	**Report Time: 1:46 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 695888** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11/1/2012
Time incident *occurred*:	**Time incident *discovered*:** 5:30 pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 11/1/2012 at approximately 5:30 pm PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date:11/1/2012	**Report Time: 8:39 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 696505** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 11-08-12	**Date incident *discovered*:** [11-8-12 9:43am]
Time incident *occurred*: 9:53am	**Time incident *discovered*:** [11-8-12 9:43am]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -

IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date 11-08-12] at approximately [9:53am] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/8/2012	**Report Time: 4:52 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 696517** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11/8/2012
Time incident *occurred*:	**Time incident *discovered*:** 10:26am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 11/8/2012 at approximately 10:26am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/8/2012	**Report Time: 6:07 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 696810** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11/13/12
Time incident occurred:	Time incident discovered: 4:10pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 11-13-12 at approximately 4:10pm PST the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/13/2012	**Report Time: 7:21 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 696996** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [November 15, 2012]
Time incident *occurred*:	**Time incident *discovered*:** [12:40 PM PST]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [November 15, 2012 at approximately [12:40 PM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 11/15/2012	**Report Time: 4:11 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #:** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:	**Report Time:**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 697261** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/19/2012	**Report Time: 1:05 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 697315** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11/19/2012 @ 4:30pm
Time incident *occurred*:	**Time incident *discovered*:** 11/19/2012 @ 4:30pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -

IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date 11-19-2012] at approximately [4:30pm] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/19/2012	**Report Time: 7:34 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 697394** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 11/20/2012	**Date incident *discovered*:** 11/20/2012
Time incident *occurred*: 10:52am	**Time incident *discovered*:** 10:52am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 11/20/2012 at approximately 10:52am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 11/20/2012	**Report Time: 2:34 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 697523** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** November 20, 2012
Time incident *occurred*:	**Time incident *discovered*:** [Fill in time Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On November 20, 2012 at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/21/2012	**Report Time: 4:47 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 697744** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11/27/2012
Time incident *occurred*:	**Time incident *discovered*:** 3:00PM PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date 11-27-2012] at approximately [3:00PM] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/27/2012	**Report Time: 6:11 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 697749** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503-230-4357	**Email address:**
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11-27-12
Time incident *occurred*:	**Time incident *discovered*:** 11-27-12

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify) Digital Camera	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date 11-27-12] at approximately [1539 Time] PST, the BPA Help Desk received a report of a missing/lost Digital Camera. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

Unknown if there were pictures of BPA property/equipment on camera.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken:	

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/27/2012	**Report Time: 7:39 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 698028** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11/30/2012
Time incident *occurred*:	**Time incident *discovered*:** 9:38 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 11/30/2012	**Report Time: 1:19 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 698601** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [12/06/12]
Time incident *occurred*:	**Time incident *discovered*:** [1050hrs]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [12/06/12] at approximately [1050] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/6/2012	**Report Time: 2:00 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 699094** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12/12/12
Time incident *occurred*:	**Time incident *discovered*:** 8:05am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On 12/12/12 at approximately 8:05 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/12/2012	**Report Time: 12:04 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 699882** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12/21/2012
Time incident *occurred*:	**Time incident *discovered*:** 12/21/2012

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 12/21/2012 at approximately 10:30am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/21/2012	**Report Time: 2:01 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 700083** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/27/2012	**Report Time: 11:54 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 700149** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12/28/2012
Time incident *occurred*:	**Time incident *discovered*:** 5:05pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 12-28-2012 at approximately 5:05pm PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken: Remote access has been disabled	

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/28/2012	**Report Time: 8:15 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 700276** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 11/01/2012	**Date incident *discovered*:** 1/02/2013
Time incident *occurred*: 8am	**Time incident *discovered*:** 7:33am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01/02/2013 at approximately 7:33am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/2/2013	**Report Time: 11:40 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 700309** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 1/2/2013
Time incident *occurred*:	**Time incident *discovered*:** 11:11 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01/02/2013 at approximately 11:11 AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/2/2013	**Report Time: 3:27 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 700377** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 01/03/13
Time incident *occurred*:	**Time incident *discovered*:** 0950hrs

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01/03/13 at approximately 0950 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/3/2013	**Report Time: 1:01 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 700392** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 01-03-2013
Time incident *occurred*:	**Time incident *discovered*:** 10:33am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On 01-03-2013 at approximately 10:33am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/3/2013	**Report Time: 2:16 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 700600** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 01/07/13
Time incident *occurred*:	**Time incident *discovered*:** 10:15 PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01/07/13 at approximately 10:15 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/7/2013	**Report Time: 1:29 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 700845** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 1/04/2013
Time incident *occurred*:	**Time incident *discovered*:** @ 8:00PM PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01/09/2013 at approximately 12:08pm PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/9/2013	**Report Time: 3:39 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 700967** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 1/10/2013
Time incident *occurred*:	**Time incident *discovered*:** 1300

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other RSA Token
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 1/10/2013 at approximately 1300 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/10/2013	**Report Time: 4:40 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 701260** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: Sean Barry	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: 503-230-3382	**Email address:** spbarry@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** 1/14/2013
Time incident *occurred*:	**Time incident *discovered*:** 6:14 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: At 6:14 PM BPA Cyber Security received a report of a stolen laptop computer. The device is not believed to stored any PII and did have whole disc encryption enabled. I don't expect any further information.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 1/14/2013	**Report Time: 9:46 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 701998 (closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 1/19/13
Time incident *occurred*:	**Time incident *discovered*:** @1400hrs

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: **Type 1 Incident / Security Category - Low**

On [01/22/2013] at approximately [1630hrs] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:
Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken
Assessment of the impact of the incident:
What actions have been taken: Webmail token has been disabled

Other Information
Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 1/22/2013	**Report Time: 7:36 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 702246** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 01/25/13
Time incident *occurred*:	**Time incident *discovered*:** 0739

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01/25/13 at approximately 0739 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 1/25/2013	**Report Time: 12:04 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 702547** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 1/29/13
Time incident *occurred*:	**Time incident *discovered*:** 9:00am PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On Tuesday 1/29/13 at about 9:00am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/29/2013	**Report Time: 1:55 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 702579** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 01/29/2013
Time incident *occurred*:	**Time incident *discovered*:** 10:00am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01/29/2013 at approximately 10:00am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/29/2013	**Report Time: 5:08 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 702594** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 01/29/13
Time incident *occurred*:	**Time incident *discovered*:** 3:40 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On 01-29-13 at approximately 3:40pm PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken: Remote access has been disabled	

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/29/2013	**Report Time: 6:46 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 702665** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 01-30-13
Time incident *occurred*:	**Time incident *discovered*:** 10am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01-30-13 at approximately 10am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 1/30/2013	**Report Time: 1:10 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 703159** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02/06/2013
Time incident *occurred*:	**Time incident *discovered*:** 08:20 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 02/06/2013 at approximately 08;20 AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/6/2013	**Report Time: 11:50 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 703160** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02/06/2013
Time incident *occurred*:	**Time incident *discovered*:** 0800

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other RSA Token
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 02/06/2013 at approximately 0800 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/6/2013	**Report Time: 12:04 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 703469** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02/08/13
Time incident *occurred*:	**Time incident *discovered*:** 1440 pst

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 02/08/13 at approximately 1440 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/8/2013	**Report Time: 5:46 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 703718** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** 2/12/13
Time incident *occurred*:	**Time incident *discovered*:** 9:09am,

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 2/12/13 at approximately 9:09 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 2/12/2013	Report Time: 1:29 PM

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 704095** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 2/15/13
Time incident *occurred*:	**Time incident *discovered*:** 1:45pst

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/15/2013	**Report Time: 5:40 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 704308** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02/19/13
Time incident *occurred*:	**Time incident *discovered*:** 9:17am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On Date 02/19/13 at approximately 9:17 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/19/2013	**Report Time: 2:12 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 704395** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02/20/2013
Time incident *occurred*:	**Time incident *discovered*:** 8:00am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other RSA Token
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 02/20/2013 at approximately 8:00am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/20/2013	**Report Time: 11:07 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 704436** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02/20/13
Time incident *occurred*:	**Time incident *discovered*:** 11:45am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 02/20/13 at approximately 11:45 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?

☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/20/2013	**Report Time: 2:47 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 705518** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 3/6/13	**Date incident *discovered*:** 3/6/13
Time incident *occurred*: 9:13 PM PST	**Time incident *discovered*:** 9:13 PM PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/7/2013	**Report Time: 10:35 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 705523** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:**
Time incident *occurred*:	**Time incident *discovered*:**

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

Tthe BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/7/2013	**Report Time: 11:21 AM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 705535** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 03/07/13
Time incident *occurred*:	**Time incident *discovered*:** 9:11am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On Date 03/07/13 at approximately 9:111am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/7/2013	**Report Time: 2:13 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 705739** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 3/09/13
Time incident *occurred*:	**Time incident *discovered*:**

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 3/11/13 at approximately 10:00 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/11/2013	**Report Time: 1:13 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 705753** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 03/11/13
Time incident *occurred*:	**Time incident *discovered*:** 11:30am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On 03/11/13 at 11:30, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken: Remote access has been disabled	

Other Information
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)
Report Information (Call Center Use Only)

Report Date: 3/11/2013	**Report Time: 2:38 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 706025** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: Sean Barry	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503-230-3382	**Email address:** spbarry@bpa.gov
Incident Information	
Date incident *occurred*: 3/14/13	**Date incident *discovered*:** 3/14/13
Time incident *occurred*: Not recorded	**Time incident *discovered*:** Not recorded

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☒ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: None	**Which critical infrastructure was affected, if any?** **None**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s): N/A	**Operating system(s) of affected machine(s):** N/A

Description of incident:
A BPA contract employee received a phone call on his BPA issued cell phone. The caller spoke in broken English and stated that his computer had not responded to a recent Windows update. The user stated that he had just used his computer and it seemed fine. The caller then repeated again that he was missing updates.

He challenged the caller stating that it was a BPA system and she was calling a BPA phone – was she from BPA. The caller then asked "This is a business phone number?" When the user replied that it was, the caller hung up.

The user and several other staff members reviewed the phone to try and determine the callers number (although it probably would have been spoofed anyway), but there was no record of the call.

Method of detection:
Personal knowledge.

IP address(es) of attackers: N/A	**Destination Port(s) and Protocol(s):** N/A
Domain name(s) of attacker(s): N/A	**Country(ies) of attacker(s):** Unknown

Suspected method of intrusion/attack:
Phone call

Suspected perpetrators and/or possible motivations:
Unknown. Social engineering – to steal credentials or get the user to visit a malicious site.

Name of Trojan(s) or malicious code(s) (if applicable): N/A	**Evidence of spoofing:** N/A

Impact and Actions Taken

Assessment of the impact of the incident:

No data was lost. No credentials were stolen.
Based on the callers reaction, it seems likely that BPA was not targeted, rather the attacker was expecting it to be a home

number and hopefully less sophisticated user. **http://blogs.msdn.com/b/securitytipstalk/archive/2010/03/09/don-t-fall-for-phony-phone-tech-support.aspx**	
What actions have been taken: This report is the only action taken.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/14/2013	**Report Time: 4:35 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 706107** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [3-15-2013]
Time incident *occurred*:	**Time incident *discovered*:** [6:56 AM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [3-15-2013] at approximately [6:56 AM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/15/2013	**Report Time: 10:25 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 706108** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [3-15-2013]
Time incident *occurred*:	**Time incident *discovered*:** [6:56 AM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☒ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [3-15-2013] at approximately [6:56 AM] PST, the BPA Help Desk received a report of a missing/lost removable media.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken
Assessment of the impact of the incident:
What actions have been taken:

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/15/2013	**Report Time: 10:43 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 706156** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 3/15/13
Time incident *occurred*:	**Time incident *discovered*:** 10:40am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

The BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/15/2013	**Report Time: 3:13 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 706349** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 3/18/13
Time incident *occurred*:	**Time incident *discovered*:** 2pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 03/18/13 at approximately 2:00pm PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/18/2013	**Report Time: 6:13 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 706350** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 3/18/13
Time incident *occurred*:	**Time incident *discovered*:** 3:30pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 03-18-13 at approximately 3:30pm PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/18/2013	**Report Time: 6:36 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 706621** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [3-20-2013]
Time incident *occurred*:	**Time incident *discovered*:** [12:34 PM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [3-20-2013] at approximately [12:34 PM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/20/2013	**Report Time: 4:46 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 706767** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 3/22/13
Time incident *occurred*:	**Time incident *discovered*:** 7:55 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 3/22/13 at approximately 7:50 am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/22/2013	**Report Time: 11:17 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 706958** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 03/26/13
Time incident *occurred*:	**Time incident *discovered*:** 1115 PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 03/26/13at approximately [1115] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/26/2013	**Report Time: 2:17 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 706985** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 3/26/13
Time incident *occurred*:	**Time incident *discovered*:** 8:00 am PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 3/26/2013	Report Time: 4:17 PM

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 707330** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 3/29/13
Time incident *occurred*:	**Time incident *discovered*:** 4:30pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/29/2013	**Report Time: 7:36 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 707972** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/9/2013	**Report Time: 10:44 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 708130** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 4-10-2013
Time incident *occurred*:	**Time incident *discovered*:** 8:20 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 4-10-2013 at approximately 8:20 AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/10/2013	**Report Time: 12:37 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 708164** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 4/10/13
Time incident *occurred*:	**Time incident *discovered*:** 11:00 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 4/10/2013	**Report Time: 3:41 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration Portland OR	**For Call Center use only:** **JC3 Ticket #: 708890** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: Dennis York	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503-230-4714	**Email address:** dryork@bpa.gov

Incident Information

Date incident *occurred*: 4/22/2013	**Date incident *discovered*:** 4/22/2013
Time incident *occurred*: 06:14	**Time incident *discovered*:** 09:30

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☒ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):** Windows XP SP3

Description of incident:
12 users clicked on links in a phishing email instructing them to reset their passwords. Two users submitted their information.

Method of detection:
I detected a large number of these phishing messages and was following up to see if any users visited the URL in the message.

IP address(es) of attackers: 195.216.243.26	**Destination Port(s) and Protocol(s):** 80
Domain name(s) of attacker(s): hxxp://weebetumeail.at.ua/1webmailupdate.html	**Country(ies) of attacker(s):** ?

Suspected method of intrusion/attack:
Phishing message

Suspected perpetrators and/or possible motivations:
Password theft

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:
Two user accounts may possibly have been compromised.

What actions have been taken:
Access to the domain has been blocked in our firewall, and the passwords for two users were changed immediately.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 4/22/2013	**Report Time: 4:24 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 709030** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 4/24/2013
Time incident *occurred*:	**Time incident *discovered*:** 12:45

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other RSA Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 4/24/2013 at approximately 12:45 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/24/2013	**Report Time: 3:52 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 709215** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident occurred:	Date incident discovered: [04-29-2013]
Time incident *occurred*:	**Time incident *discovered*:** [4:36AM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On [04-29-2013] at approximately [4:36AM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/29/2013	**Report Time: 9:50 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 709445** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05/01/13
Time incident *occurred*:	**Time incident *discovered*:** 2:34 pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05/01/13 at approximately 1:45 pm PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/1/2013	**Report Time: 6:08 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 709644** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 5/6/13
Time incident *occurred*:	**Time incident *discovered*:** 7:30 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 5/6/13 at approximately 7:30 am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/6/2013	**Report Time: 10:40 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 709882** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05-09-2013
Time incident *occurred*:	**Time incident *discovered*:** 09:20 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/9/2013	**Report Time: 12:37 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 710049** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 05/09/13	**Date incident *discovered*:** 05/10/13
Time incident *occurred*: 7pm PST	**Time incident *discovered*:** 1:39 pm PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05/10/13 at approximately 1:39pm PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:5/10/2013	**Report Time: 4:55 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 710173** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05/14/13
Time incident *occurred*:	**Time incident *discovered*:** 1000hrs PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☒ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 5/14/13 at approximately 1000 PST, the BPA Help Desk received a report of a missing/lost removable media.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/14/2013	**Report Time: 1:12 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 710175** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 5/14/13
Time incident *occurred*:	**Time incident *discovered*:** 10:15am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☒ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 5/14/13 at approximately 10:15am PST, the BPA Help Desk received a report of a missing/lost removable media.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/14/2013	**Report Time: 1:24 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 710295** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 05-14-2013	**Date incident *discovered*:** 05-14-2013
Time incident *occurred*: 7:00am	**Time incident *discovered*:** 7:00am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05-15-13 at approximately 7:44 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/15/2013	**Report Time: 10:45 am ET**

From: JC3 <CIRC@JC3.DOE.GOV>
Sent: Monday, May 20, 2013 7:45 AM
To: JC3
Cc: McCann,April A (BPA) - NJB-B1; Prouse,Gary L (BPA) - NJB-B1; Barry,Sean P (BPA) - NJB-B1
Subject: JC3-710592 INCIDENT REPORT - Missing/Lost Blackberry Smart phone

To Whom It May Concern,

The attached information was reported to JC3 on 5/20/2013 at 10:22 AM ET. The JC3 has assigned ticket number JC3-710592 to this Incident. Please reference this ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

Carla Ellerbe
U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3 Call Center
1-866-941-2472
circ@jc3.doe.gov

From: Roberts,Ethan E (CONTR) - NJRH-2 [mailto:eeroberts@bpa.gov] On Behalf Of Help Desk
Sent: Monday, May 20, 2013 10:22 AM
To: JC3
Cc: Cyber Security; Help Desk; McCann,April A (BPA) - NJB-B1; Prouse,Gary L (BPA) - NJB-B1; Barry, Sean
Subject: INCIDENT REPORT - Missing/Lost Blackberry Smart phone

Type 1 Incident / Security Category - Low
On 5/20/13 at approximately 7 am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 710624** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05/20/13
Time incident *occurred*:	**Time incident *discovered*:** 1400 PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05/20/13 at approximately 1400 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/20/2013	**Report Time: 5:11 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 711884 (Closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 6/11/13
Time incident *occurred*:	**Time incident *discovered*:** 4:15pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 6/11/13 at approximately 4:15 PST,, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken: Webmail token has been disabled	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:6/11/2013	**Report Time: 7:37 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 711937** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 06-12-13
Time incident *occurred*:	**Time incident *discovered*:** 10:21 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 06-12-13 at approximately 10:21 AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 6/12/2013	**Report Time: 3:23 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 712303** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 06/20/13
Time incident *occurred*:	**Time incident *discovered*:** 3:00

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 06-20-13 at approximately 3:00 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Thu 6/20/2013	**Report Time: 6:12 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 712319** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 6/20/2013	**Date incident *discovered*:** 6/20/2013
Time incident *occurred*:	**Time incident *discovered*:** 3pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 6/20/2013 at approximately 3:00pm PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 6/20/2013	**Report Time: 7:36 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 712444** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 6/24/13
Time incident *occurred*:	**Time incident *discovered*:** 10:43

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 6/24/13 at approximately 10:43 AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Mon 6/24/2013	**Report Time: 2:22 PM EST**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 712554** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 6/25/13
Time incident *occurred*:	**Time incident *discovered*:** 11am PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 6/25/13 at approximately 11am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Tue 6/25/2013	**Report Time: 3:52 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 712736** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 6/27/13
Time incident *occurred*:	**Time incident *discovered*:** Unspecified

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ PDA
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 6/27/13, the BPA Help Desk received a report of a missing/lost removable media.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken
Assessment of the impact of the incident:
What actions have been taken:

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Thu 6/27/2013	**Report Time: 5:36 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 712809** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 6/28/13
Time incident *occurred*:	**Time incident *discovered*:** 2:43pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 6/28/13 at approximately 2:43 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Fri 6/28/2013	**Report Time: 6:32 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 712847** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 07-01-13
Time incident *occurred*:	**Time incident *discovered*:** 07:40 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 07-01-13 at approximately 07:40 AM PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Mon 7/1/2013	**Report Time: 11:18 AM** ET

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 712948** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 7/2/13
Time incident *occurred*:	**Time incident *discovered*:** 10am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 7/2/13 at approximately 10am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Tue 7/2/2013	**Report Time: 1:13 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 713180** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 07-06-13
Time incident *occurred*:	**Time incident *discovered*:** 2:26 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 07-06-13 at approximately 2:26 PM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 7/8/2013	**Report Time: 9:49 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 713277** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 6/20/13
Time incident *occurred*:	**Time incident *discovered*:** 3:30 pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 6/20/2013 at approximately 3:30pm PST, BPA received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 7/9/2013	**Report Time: 2:22 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 713499** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 07/11/13
Time incident *occurred*:	**Time incident *discovered*:** 1600hrs PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 07/11/13 at approximately 1600 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Thu 7/11/2013	**Report Time: 7:19 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 713692** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 7/16/13
Time incident *occurred*:	**Time incident *discovered*:** 10:30 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: 1	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 7/16/13 at approximately 10:30am PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Tue 7/16/2013 4:16 PM	**Report Time: 4:16 PM EST**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 713693** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [July 16, 2013]
Time incident *occurred*:	**Time incident *discovered*:** [11:30 a.m. PST]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [07-16-2013] at approximately [11:30 a.m.] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: Tue 7/16/2013	**Report Time: 4:31 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 713713** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [07/16/13]
Time incident *occurred*:	**Time incident *discovered*:** [1600pst]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [07/16/13] at approximately [1600] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Tue 7/16/2013	**Report Time: 7:09 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 713803** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 7/17/2013
Time incident *occurred*:	**Time incident *discovered*:** 5:20 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 7/17/2013	**Report Time: 8:30 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 714526** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 7/31/2013
Time incident *occurred*:	**Time incident *discovered*:** 2:43p

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 7/31/2013 at approximately 2:43p PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Wed 7/31/2013	**Report Time: 8:11 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 714562** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 08/01/13
Time incident *occurred*:	**Time incident *discovered*:** 0845hrs PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 08/01/13 at approximately 0845 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/1/2013	**Report Time: 11:53 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 714645** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 08-02-2013
Time incident *occurred*:	**Time incident *discovered*:** 12:15pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/2/2013	**Report Time: 3:26 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 714874** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 8/ 7/ 13
Time incident *occurred*:	**Time incident *discovered*:** Noon

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 8/ 7/ 13 at approximately Noon PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/7/2013	**Report Time: 3:25 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 715182** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** August 12, 2013
Time incident *occurred*:	**Time incident *discovered*:** 10.03am PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On August 12, 2013 at approximately 10.03am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/12/2013	**Report Time: 1:08 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 715821** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 08-21-13
Time incident *occurred*:	**Time incident *discovered*:** 2:00pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Wed 8/21/2013	**Report Time: 6:57 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 716184** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 8/27
Time incident *occurred*:	**Time incident *discovered*:** 1:30

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 8/27/13 at approximately 2:00pm PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/27/2013	**Report Time: 5:21 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 716261** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 08/28/13
Time incident *occurred*:	**Time incident *discovered*:** 10am PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 08/28/13 at approximately 10am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/28/2013	**Report Time: 1:09 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 716316** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 8/29/13	**Date incident *discovered*:** 8/29/13
Time incident *occurred*: 8:46am	**Time incident *discovered*:** 8:46

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 8/29/13 at approximately 8:46am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/29/2013	**Report Time: 11:52 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 716325** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 8/29/2013	**Date incident *discovered*:** 8/29/2013
Time incident *occurred*: 8:30am	**Time incident *discovered*:** 9:28am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 08-29-13 at approximately 9:28am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/29/2013	**Report Time: 12:38 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 716420** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 8/30/13
Time incident *occurred*:	**Time incident *discovered*:** Unknown

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 8/30/13 at approximately 11:30am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 8/30/2013	**Report Time: 5:23 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 716463** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 9/3/13
Time incident *occurred*:	**Time incident *discovered*:** 11:00 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 9/3/13 at approximately 11anm PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken: Remote access has been disabled	

Other Information
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)
Report Information (Call Center Use Only)

Report Date: 9/3/2013	**Report Time: 2:09 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 716470** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 09/03/13
Time incident *occurred*:	**Time incident *discovered*:** 12:50 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On 09/03/13 at approximately 12:50 PM PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)
Report Information (Call Center Use Only)

Report Date: 9/3/2013	**Report Time: 4:22 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 716778** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [9/6/13]
Time incident *occurred*:	**Time incident *discovered*:** [11:49 AM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [09-06-13] at approximately [11:49 AM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 9/9/2013	**Report Time: 2:29 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 716976** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 9/11/2013	**Date incident *discovered*:** 9/11/2013
Time incident *occurred*: 2:00 pm	**Time incident *discovered*:** 2:45 pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 09-11-2013 at approximately 2:45pm PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 9/11/2013	**Report Time: 5:56 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 717200** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [09-16-2013]
Time incident *occurred*:	**Time incident *discovered*:** [3:45 PM PST]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [09-16-2013] at approximately [3:45 PM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 9/16/2013	**Report Time: 6:57 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 717229** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 09-17-2013
Time incident *occurred*:	**Time incident *discovered*:** 9:45am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 9/17/2013	**Report Time: 12:55 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 717233** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 9/17/2013
Time incident *occurred*:	**Time incident *discovered*:** 10:10am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 09/17/13 at approximately 10:10am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 9/17/2013	**Report Time: 1:19 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 717597** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 09-24-2013
Time incident *occurred*:	**Time incident *discovered*:** 6:15 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☒ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost removable media.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 9/24/2013	**Report Time: 1:04 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718059** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10-01-2013
Time incident *occurred*:	**Time incident *discovered*:** 3:00 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/1/2013	**Report Time: 6:10 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718093** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 09/30/13
Time incident *occurred*:	**Time incident *discovered*:** ??:?? AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/02/13 at approximately 11:30 AM PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/2/2013	**Report Time: 2:48 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718200** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/3/13
Time incident *occurred*:	**Time incident *discovered*:** 1:00pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/3/13 at approximately 1:00 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/3/2013	**Report Time: 4:04 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718377** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/7/13
Time incident *occurred*:	**Time incident *discovered*:** 1pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/7/13 at approximately 1pm PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/7/2013	**Report Time: 3:49 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718400** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [October 8, 2013]
Time incident *occurred*:	**Time incident *discovered*:** [8:07 AM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [October 8, 2013] at approximately [8:07AM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/8/2013	**Report Time: 11:32 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718430** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/08/2013 1:16 PM
Time incident *occurred*:	**Time incident *discovered*:** 10/04/2013 unknown AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/08/13 at approximately ??:?? AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/8/2013	**Report Time: 4:29 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718549** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/09/13
Time incident *occurred*:	**Time incident *discovered*:** 1600PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/09/13 at approximately 1600 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Wed 10/9/2013	**Report Time: 7:18 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718563** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/09/13
Time incident *occurred*:	**Time incident *discovered*:** 5:45PM PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/09/13 at approximately 5:45PM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Wed 10/9/2013	**Report Time: 8:58 PM** ET

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718830** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/16/2013	**Report Time: 5:07 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718843** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Wed 10/16/2013	**Report Time: 7:11 PM** ET

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718913** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 10/16/2013	**Date incident *discovered*:** 10/16/2013
Time incident *occurred*: 10:16	**Time incident *discovered*:** 10:16

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/17/2013 at approximately 1:06pm PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/17/2013	**Report Time: 4:13 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718966** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/18/2013
Time incident *occurred*:	**Time incident *discovered*:** 05:47 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On Date 10-18-13 at approximately 05:47 AM PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/18/2013	**Report Time: 9:42 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 718978** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 10-17-2013	**Date incident *discovered*:** 10/18/2013
Time incident *occurred*: 5.00 pm	**Time incident *discovered*:** 7:36am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10-18*-2013 at approximately 7:36am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/18/2013	**Report Time: 10:44 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 719102** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10-21-2013
Time incident *occurred*:	**Time incident *discovered*:** 3:30pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/21/2013	**Report Time: 6:43 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 719163** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/20/2013
Time incident *occurred*:	**Time incident *discovered*:** In the morning

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other Blackberry Curve
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/22/2013 at approximately 10:00 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/22/2013	**Report Time: 1:30 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 719354** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10-24-2013
Time incident *occurred*:	**Time incident *discovered*:** 2:40pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/24/2013	**Report Time: 5:49 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 719408** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/25/2013	**Report Time: 1:38 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 719528** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/28/13
Time incident *occurred*:	**Time incident *discovered*:** 10:45am PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 10/28/13 at approximately 10:45am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/28/2013	**Report Time: 1:50 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 719610** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 10/29/13
Time incident *occurred*:	**Time incident *discovered*:** 1500PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [10/29/13] at approximately [1500] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 10/29/2013	**Report Time: 6:07 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 719958** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11-06-2013
Time incident *occurred*:	**Time incident *discovered*:** 9:55am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/6/2013	**Report Time: 1:04 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 720305** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Unknown 11-10-13?	11/13/13
Time incident *occurred*:	**Time incident *discovered*:** 10:06

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 11/13/13 @10:06, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/13/2013	**Report Time: 1:10 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 720334** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11/13/13
Time incident *occurred*:	**Time incident *discovered*:** 17:30

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On Date 11/13/13 at approximately 17:30 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Wed 11/13/2013	**Report Time: 8:57 PM** ET

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 720366** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11/14/13
Time incident *occurred*:	**Time incident *discovered*:** 9:35PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 11/14/13 at approximately 9:35 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/14/2013	**Report Time: 1:27 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 720693** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11/20/2013
Time incident *occurred*:	**Time incident *discovered*:** 3:45pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Wed 11/20/2013	**Report Time: 7:06 PM** ET

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 720760** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11-21-2013
Time incident *occurred*:	**Time incident *discovered*:** 2:00pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/21/2013	**Report Time: 5:35 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 720806** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 11/04/2013	**Date incident *discovered*:** 11/04/2013
Time incident *occurred*: unknown	**Time incident *discovered*:** unknown

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 11/22/2013 at approximately 10:30a, PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/22/2013	**Report Time: 1:52 PM ET**

OFFICIAL USE ONLY

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 720907** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 11/25/13
Time incident *occurred*:	**Time incident *discovered*:** 12:30 pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 11/25/13 at approximately 12:30pm PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 11/25/2013	**Report Time: 3:40 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #:** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 12/2/13	**Date incident *discovered*:** 12/3/13
Time incident *occurred*: 3:00pm	**Time incident *discovered*:** 6:46am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 12-3-2013 at approximately 6:46am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:	**Report Time:**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 721171** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: Sean Barry	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503-230-3382	**Email address:** spbarry@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12/3/2013
Time incident *occurred*:	**Time incident *discovered*:** 1615

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☒ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☒ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: None	**Which critical infrastructure was affected, if any?** **None**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? 8 Have the individuals been notified? No Was the PII of Contractors or Federal employees? Yes
IP address of affected machine(s): N/A	**Operating system(s) of affected machine(s):** N/A

Description of incident:
In responding to a FOIA request from Dan Seligman (BPAWatch.com) some un-redacted documents were inadvertently sent. At this time, I believe it is only names – but within the context of the meeting notes and other documentation related to our ongoing issues in HCM.
7 First/Last names of BPA employees (current and former) and TVA employee
1 First name of BPA employee
1 personal cell phone number, e-mail address and home address of current BPA employee

Method of detection:

IP address(es) of attackers: N/A	**Destination Port(s) and Protocol(s):** N/A
Domain name(s) of attacker(s): N/A	**Country(ies) of attacker(s):** N/A
Suspected method of intrusion/attack: N/A	
Suspected perpetrators and/or possible motivations: N/A	
Name of Trojan(s) or malicious code(s) (if applicable): N/A	**Evidence of spoofing:** N/A

Impact and Actions Taken

Assessment of the impact of the incident:
TBD

What actions have been taken:
BPA FOIA Office:
1) Asked for unredacted document back from recipient. 2) Reported to BPA Privacy Act Officer, BPA Office of Cyber Security, BPA Office of General Counsel (FOIA/Privacy attorneys), and DOE Privacy Officer (voice mail) and BPA acting Administrator (voice mail).

BPA Office of Cyber Security Office: 1) Reported to JC3 CIRC. 2) Notified BPA CISO (e-mail). 3) Logged event.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:12/3/2013	**Report Time:8:15 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 721269** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12/04/2013
Time incident *occurred*:	**Time incident *discovered*:** 3:15pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/4/2013	**Report Time: 6:27 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 721521** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 1:20 PM 12/9/2013	**Date incident *discovered*:** [1:20 PM 12/9/2013]
Time incident *occurred*: 1:20 PM 12/9/2013	**Time incident *discovered*:** [1:20 PM 12/9/2013]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/9/2013	**Report Time: 5:14 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 721602** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12/11/13
Time incident *occurred*:	**Time incident *discovered*:** 08:24 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 12/11/13 at approximately 08:24 AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/11/2013	**Report Time: 12:05 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 721603** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12/11/13
Time incident *occurred*:	**Time incident *discovered*:** 08:24 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

<u>Type 1 Incident / Security Category - Low</u>

On 12/11/13 at approximately 08:24 AM PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)
Report Information (Call Center Use Only)

Report Date: 12/11/2013	**Report Time: 12:31 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 721824** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12/17/13
Time incident *occurred*:	**Time incident *discovered*:** 1029PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 12/17/13 at approximately 1029 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/17/2013	**Report Time: 1:30 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 721836** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12/17/13
Time incident *occurred*:	**Time incident *discovered*:** 11:45 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 12/17/13 at approximately 11:45 PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)
Report Information (Call Center Use Only)

Report Date: 12/17/2013	**Report Time: 3:25 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 721951** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [12-19-2013]
Time incident *occurred*:	**Time incident *discovered*:** [1:55 PM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [12-19-2013] at approximately [1:55PM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/19/2013	**Report Time: 5:11 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 722083** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*: Undetermined	**Date incident *discovered*:** December 23, 2013
Time incident *occurred*: Undetermined	**Time incident *discovered*:** 9:55 a.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
X Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s): careers.bpa.gov / transmission.bpa.gov	**Operating system(s) of affected machine(s):**

Description of incident:
Unauthorized file posted to BPA public facing websites

Method of detection:
Reported by BPA IT personnel

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Web sites have been taken down. Reviewing logs to determine compromise.
CI has been notified of this incident.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date:12/23/2013	**Report Time:8:01 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 722318** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12/31/2013
Time incident *occurred*:	**Time incident *discovered*:** 09:00 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 12-31-13 at approximately 9:00 AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/31/2013	**Report Time: 1:32 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 722324** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 12-31-13
Time incident *occurred*:	**Time incident *discovered*:** 11:55 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 12-31-13] at approximately 11:55 AM PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 12/31/2013	**Report Time: 2:58 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 722415** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [January 3, 2014]
Time incident *occurred*:	**Time incident *discovered*:** [8:50AM PST]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [01-03-2014] at approximately [8:50AM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/3/2014	**Report Time: 12:09 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 722553** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken
Assessment of the impact of the incident:
What actions have been taken: Webmail token has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/6/2014	**Report Time: 6:11 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 722654** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 01-07-2014
Time incident *occurred*:	**Time incident *discovered*:** 10:20 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/8/2014	**Report Time: 11:24 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 722678** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 12-24-13	**Date incident *discovered*:** 01/08/14
Time incident *occurred*: 3:00pm	**Time incident *discovered*:** 12:27pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

The BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/8/2014	**Report Time: 3:28 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 722915** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 1/13/14 @5:00PM
Time incident *occurred*:	**Time incident *discovered*:** 1/14/14 @8:54M

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01/14/14 at approximately 8:54AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/14/2014	**Report Time: 11:56 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 722973** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 01/14/14
Time incident *occurred*:	**Time incident *discovered*:** 1400 PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01/14/14 at approximately 1400 PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/14/2014	**Report Time: 5:16 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #:** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 01/24/14	**Date incident *discovered*:** 01/27/14
Time incident *occurred*: 5:30pm	**Time incident *discovered*:** 7:09am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:	**Report Time:**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 723673** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 01/28/14
Time incident *occurred*:	**Time incident *discovered*:** 12:20 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 01/28/14 at approximately 12:20 PM PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 1/28/2014	**Report Time: 4:30 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 723999** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02-04-2014
Time incident *occurred*:	**Time incident *discovered*:** 4:45pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)
Report Information (Call Center Use Only)

Report Date:2/4/2014	**Report Time: 8:00 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 724070** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 2/6/2014
Time incident *occurred*:	**Time incident *discovered*:** 7:37

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 02/06/14 at approximately 7:37 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/6/2014	**Report Time: 10:39 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 724230** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 2/7/2014	**Date incident *discovered*:** 2/10/2014
Time incident *occurred*:	**Time incident *discovered*:** 2:05pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 02-10-14 at approximately 2:05pm PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:2/10/14	**Report Time: 5:08 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 724240** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02-10-2014
Time incident *occurred*:	**Time incident *discovered*:** 1:25 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/10/2014	**Report Time: 6:05 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 724346** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 2/12/14 at approximately 9:30 PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)
Report Information (Call Center Use Only)

Report Date: 2/12/2014	**Report Time: 12:44 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 724655** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02-18-2014
Time incident *occurred*:	**Time incident *discovered*:** 7:33

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 02-18-2014 at approximately 7:33PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/18/2014	**Report Time: 10:36 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 724665** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/18/2014	**Report Time: 12:19 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 724738** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [02-10-2014] at approximately [8am] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/19/2014	**Report Time: 11:28 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 724903** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 02-20-2014
Time incident *occurred*:	**Time incident *discovered*:** 12:26PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: 0	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Thu 2/20/2014	**Report Time: 8:07 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 724952** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 2/21/14
Time incident *occurred*:	**Time incident *discovered*:** 11:05am PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On Date 02/21/14 at approximately 11:05am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/21/2014	**Report Time: 2:50 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 725094** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 2/23/14
Time incident *occurred*:	**Time incident *discovered*:** Night

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 2/24/14 at approximately 11am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 2/24/2014	**Report Time: 2:16 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 725238** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 2/26/14
Time incident *occurred*:	**Time incident *discovered*:** 2/26/14

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 2/26/14 at approximately 12pm PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)
Report Information (Call Center Use Only)

Report Date: 2/26/2014	**Report Time: 3:29 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 725429** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 3/3/14
Time incident *occurred*:	**Time incident *discovered*:** 7:30 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 3/3/14 at approximately 7:30 AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/3/2014	**Report Time: 10:43 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 725581** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [March 6, 2014]
Time incident *occurred*:	**Time incident *discovered*:** [8:19AM PST]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [03-06-2014] at approximately [8:19AM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/6/2014	**Report Time: 11:35 am ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 725588** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 03/06/14
Time incident *occurred*:	**Time incident *discovered*:** 8:55am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 03/06/14 at approximately 8:55am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/6/2014	**Report Time: 12:00 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 725877** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [03/13/14]
Time incident *occurred*:	**Time incident *discovered*:** [0900 PST]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [03/13/14] at approximately [0900] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/13/2014	**Report Time: 12:23 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 726157** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 3/19/14
Time incident *occurred*:	**Time incident *discovered*:** 9am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 3/19/14 at approximately 9am PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/19/2014	**Report Time: 12:25 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 726297** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 03-21-2014
Time incident *occurred*:	**Time incident *discovered*:** 8:25 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 03-21-2014 at approximately 8:25AM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/21/2014	**Report Time: 2:21 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 726768** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 04/02/14
Time incident *occurred*:	**Time incident *discovered*:** 12:38 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 04/02/14 at approximately 12:38 PM PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Wed 4/2/2014	**Report Time: 3:53 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 726976** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 04/02/14
Time incident *occurred*:	**Time incident *discovered*:** 6:00 p.m.

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: 2	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 04/02/14 at approximately 6:00 PST, the BPA Office of Cyber Security received a report of two missing/lost laptop computers. There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/2/2014	**Report Time: 9:22 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 727015** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 04/03/14
Time incident *occurred*:	**Time incident *discovered*:** 1:27 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 04/03/14 at approximately 1:27 PM PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Thu 4/3/2014	**Report Time: 5:32 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 727093** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 4/4/14
Time incident *occurred*:	**Time incident *discovered*:** 3:00 pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 04/04/14 at approximately 3:00 pm PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:
Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken
Assessment of the impact of the incident:
What actions have been taken:
Webmail token has been disabled

Other Information
Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: Fri 4/4/2014	**Report Time: 6:00 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 727371** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [04-10-2014]
Time incident *occurred*:	**Time incident *discovered*:** [7:57 AM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [4/10/2014] at approximately [7:57 AM] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/10/2014	**Report Time: 11:11 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 727450** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 04/10/11
Time incident *occurred*:	**Time incident *discovered*:** 10am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 04/11/14 at approximately 9am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/11/2014	**Report Time: 12:13 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 727555** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 04-14-2014
Time incident *occurred*:	**Time incident *discovered*:** 10:00 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Mon 4/14/2014	**Report Time: 2:22 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 727583** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 04/14/14
Time incident *occurred*:	**Time incident *discovered*:** 1400hrs PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 04-14-14 at approximately 1400 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken:	

Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/14/2014	**Report Time: 5:03 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 727647** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 04/15/14
Time incident *occurred*:	**Time incident *discovered*:** 7:45 AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 04/15/14 at approximately 7:45 AM PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Tue 4/15/2014	**Report Time: 11:54 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 727864** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [4/17/2014]
Time incident *occurred*:	**Time incident *discovered*:** [1:48 PM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/17/2014	**Report Time: 4:59 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 727907** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 4/18/14
Time incident *occurred*:	**Time incident *discovered*:** 8am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 4/18/14 at approximately 8am PST, the BPA Help Desk received a report of a missing/lost cell phone (Not a Blackberry). The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. BPA does not allow files to be downloaded and locally stored. The device is used for phone purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	

Assessment of the impact of the incident:	
What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/18/2014	**Report Time: 11:18 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 728098** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 04-21-14
Time incident *occurred*:	**Time incident *discovered*:** 09:00

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 04-21-14 at approximately 09:00 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken:	

Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/21/2014	**Report Time: 12:56 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 728265** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 04/18/2014	**Date incident *discovered*:** 04/23/2014
Time incident *occurred*: 11:41	**Time incident *discovered*:** 11:41

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 04/23/14 at approximately 11:41 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 4/23/2014	**Report Time: 2:45 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 728552** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [4/26/2014]
Time incident *occurred*:	**Time incident *discovered*:** [8:00 PM]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [4/26/2014] at approximately [8:00PM] PST the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:4/28/2014	**Report Time:6:28 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 728887** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05/01/14
Time incident *occurred*:	**Time incident *discovered*:** 12:56 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low
On 05-01-14 at approximately 12:56 PM PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Smartphone has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/1/2014	**Report Time: 4:15 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 728895** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05-01-2014
Time incident *occurred*:	**Time incident *discovered*:** 2pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date 05-01-14] at approximately [3:23 PM] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/1/2014	**Report Time: 5:23 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 728943** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05-02-2014
Time incident *occurred*:	**Time incident *discovered*:** 12:20pm

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05-02-2014 at approximately 12:20pm PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/2/2014	**Report Time: 3:26 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 729035** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05-05-2014
Time incident *occurred*:	**Time incident *discovered*:** 9:45am pst

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05-05-14 at approximately 9:45am PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment-Pointsec.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/5/2014	**Report Time: 1:07 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 729** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05/05/14
Time incident *occurred*:	**Time incident *discovered*:** 1:42

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: 0	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05-05-14 at approximately 1:42 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/5/2014	**Report Time: 4:47 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 729103** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** 05-06-2014
Time incident *occurred*:	**Time incident *discovered*:** 07:50 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☒ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05-06-2014 at approximately 07:50 PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer. This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 5/6/2014	**Report Time: 11:07 AM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 729147** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*: 5/6/2014	**Date incident *discovered*:** 5/6/2014
Time incident *occurred*: 7:00 AM	**Time incident *discovered*:** 12:55 PM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [5/6/2014] at approximately [12:55 PM] PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes. This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Smartphone has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/6/2014	**Report Time: 4:05 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 729164** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05-06-14
Time incident *occurred*:	**Time incident *discovered*:** 13:40

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☒ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05-06-14 at approximately 13:40 PST, the BPA Help Desk received a report of a missing/lost laptop computer. The appropriate staff has been notified to disable remote access and to revoke the VPN certificate.

There was no known PII or SUI information on the computer.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Remote access has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/6/2014	**Report Time: 5:51 PM**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 729589** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05-14-14
Time incident *occurred*:	**Time incident *discovered*:** 4:00 pm PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05-14-14 at approximately 4:00pm PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Wed 5/14/2014	**Report Time: 7:01 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 729620** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 05-15-14
Time incident *occurred*:	**Time incident *discovered*:** 9:20am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05-15-14 at approximately 9:20am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken: Smartphone has been disabled.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/15/2014	**Report Time: 12:22 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 729858** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 5/20/14
Time incident *occurred*:	**Time incident *discovered*:** 8:29 am PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 05/20/14 at approximately 8:29 PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/20/2014	**Report Time: 11:31 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 729877** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 5-20-2014
Time incident *occurred*:	**Time incident *discovered*:** 10:50am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/20/2014	**Report Time: 1:55 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 729933** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [5/21/14]
Time incident *occurred*:	**Time incident *discovered*:** [1300 PST]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low
On 5/21/14 at approximately 1300 PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken: Smartphone has been disabled.	

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/21/2014	**Report Time: 4:39 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 730066** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** PA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** [Fill in **date** Help Desk notified]
Time incident *occurred*:	**Time incident *discovered*:** [Fill in **time** Help Desk notified]

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On [Date MM-DD-YY] at approximately [Time] PST, the BPA Help Desk received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Thu 5/22/2014	**Report Time: 6:51 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 730396** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: BPA Help Desk	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503 230-4357	**Email address:** helpdesk@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** 5/30/14
Time incident *occurred*:	**Time incident *discovered*:** 8 am

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On 5/30/14 at approximately 8 am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes. This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Smartphone has been disabled.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 5/30/2014	**Report Time: 11:37 AM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 730430 (Update 1)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: Sean Barry	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 503-230-3382	**Email address:** spbarry@bpa.gov
Incident Information	
Date incident *occurred*: Unknown	**Date incident *discovered*:** 5/30/14
Time incident *occurred*: Unknown	**Time incident *discovered*:** 14:42

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☒ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☒ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: N/A	**Which critical infrastructure was affected, if any?** **N/A**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? 99 Have the individuals been notified? No Was the PII of Contractors or Federal employees? Believed to be contractors
IP address of affected machine(s): N/A	**Operating system(s) of affected machine(s):** N/A

Description of incident:
Social Security Numbers posted to widely viewable SharePoint site.

Update 1: This case can be closed. It was confirmed to be dummy data that was a part of a training course a BPA employee had taken.

Method of detection:
Internal search. "I found a list of personnel social security numbers by entering "social security number" into the SharePoint search bar. The very first link returned to me was a document (on SP) containing last names SS#s of around 100 personnel. Given that you and I can see it, it's safe to say that it's viewable by all BPA."

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Report to JC3-CIRC

To be done: Remove list. Determine how it was posted. Determine whether or not they are actual people/SSNs or if this is some sort

of training document.	
Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: Fri 5/30/2014	**Report Time: 6:50 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer
Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report

Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 672456 Closed** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** January 4, 2012
Time incident *occurred*:	**Time incident *discovered*:** 3:45 p.m. PST

Type 1 Incident:

System Compromise/Intrusion
- ☐ Root Compromise ☐ User Compromise

Loss, Theft, or Missing
- ☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA token)

Malicious Code
- ☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)

☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IMI Category:
☐ IMI1- ☐ IMI2- ☐ IMI3- ☐ IMI4-

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On January 4, 2012 at 3:45 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 1/4/2012	**Report Time: 7:39 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer
Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report

Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 672643** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** January 6, 2012
Time incident *occurred*:	**Time incident *discovered*:** 10:25 a.m. PST

Type 1 Incident:

System Compromise/Intrusion
- ☐ Root Compromise ☐ User Compromise

Loss, Theft, or Missing
- ☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA TOKEN)

Malicious Code
- ☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)

☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IMI Category:
☐ IMI1- ☐ IMI2- ☐ IMI3- ☐ IMI4-

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: N/A	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On January 6, 2012 at 10:25 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 1/6/2012	**Report Time: 2:19 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer
Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report

Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 672669** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** January 6, 2012
Time incident *occurred*:	**Time incident *discovered*:** 2:05 p.m. PST

Type 1 Incident:

System Compromise/Intrusion
- ☐ Root Compromise ☐ User Compromise

Loss, Theft, or Missing
- ☐ Desktop ☐ Laptop ☐ Media ☒ Other (Phone)

Malicious Code
- ☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)

☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IMI Category:
☐ IMI1- ☐ IMI2- ☐ IMI3- ☐ IMI4-

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: N/A	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On January 6, 2012 at approximately 2:05 p.m. PST, the Office of Cyber Security received a report of a stolen Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.

There was no known PII or SUI information on the device.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:

Blackberry service has been terminated

Other Information

Who has been notified?

☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 1/6/2012	**Report Time: 5:51 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer
Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report

Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 673181** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*: UNK	**Date incident *discovered*:** January 13, 2012
Time incident *occurred*:	**Time incident *discovered*:** 6:15 p.m. PST

Type 1 Incident:

System Compromise/Intrusion
- ☐ Root Compromise ☐ User Compromise

Loss, Theft, or Missing
- ☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)

Malicious Code
- ☐ Trojan ☐ Virus ☐ Worm ☒ Other (Webmail token)

☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IMI Category:
☐ IMI1- ☐ IMI2- ☐ IMI3- ☐ IMI4-

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: N/A	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On January 13, 2012 at 6:15 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date:1/13/2012	Report Time: 9:57 PM ET

JC3-CIRC 10.2011 v.6

U.S. Department of Energy
Office of the Chief Information Officer
Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report

Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 673368** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** January 19, 2012
Time incident *occurred*:	**Time incident *discovered*:** 12:15 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IMI Category:
☐ IMI1- ☐ IMI2- ☐ IMI3- ☐ IMI4-

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident: On January 19, 2012 at 12:15 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled. We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: Thu 1/19/2012	**Report Time: 4:07PM ET**

JC3-CIRC 10.2011 v.6

U.S. Department of Energy
Office of the Chief Information Officer
Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report

Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 674717** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** February 13, 2012
Time incident *occurred*:	**Time incident *discovered*:** 1:07 p.m. PST

Type 1 Incident:

System Compromise/Intrusion
- ☐ Root Compromise ☐ User Compromise

Loss, Theft, or Missing
- ☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA webmail token)

Malicious Code
- ☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)

☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IMI Category:
☐ IMI1- ☐ IMI2- ☐ IMI3- ☐ IMI4-

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On February 13, 2012 at 1:07 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Webmail token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 2/13/2012	**Report Time: 7:32 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #:** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** February 24, 2012
Time incident *occurred*:	**Time incident *discovered*:** 4:00 p.m. PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

Type 1 Incident / Security Category - Low

On February 24, 2012 at approximately 4:00 p.m. PST, the BPA Office of Cyber Security was notified that two BPA internal server names (**SPNPS0105.bud.bpa.gov and PIHS005.bud.bpa.gov)** were accidentally posted/published to the Microsoft's Script Center's Technet Site - http://gallery.technet.microsoft.com/scriptcenter/SCOM-Agent-Installation-8c237afe

A request has been sent to Microsoft to remove this information from the website.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Request sent to Microsoft to delete information from the website posting.

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:	**Report Time:**

OFFICIAL USE ONLY

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 675633** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** February 29, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:34 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (Blackberry)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: 1	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On February 29, 2012 at approximately 11:34 a.m. PST, the Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.

There was no known PII or SUI information on the device.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**
Impact and Actions Taken	
Assessment of the impact of the incident:	
What actions have been taken:	
Other Information	

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 2/29/2012	**Report Time: 3:25 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: BPA	**For Call Center use only:** **JC3-CIRC Ticket #: 675841** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: Sean Barry	**Program Office Name (NNSA, SC, EM, etc.):** BPA
Phone #: 502-230-3382	**Email address:** spbarry@bpa.gov

Incident Information

Date incident *occurred*: 3/2/2012	**Date incident *discovered*:** 3/2/2012
Time incident *occurred*:	**Time incident *discovered*:** 8AM

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☒ Desktop ☐ Laptop ☐ Media ☒ Other - Blackberry
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: 2	**Which critical infrastructure was affected, if any?** **None**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Yes Was the drive(s) or file(s) password protected? Yes Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
Laptop and phone stolen from employees car, parked outside her residence over night. On March 2, 2012 at approximately 8:15 a.m. PST, the Office of Cyber Security received a report of a stolen laptop and Blackberry smartphone. There was no known sensitive PII or SUI information on the computer. Whole disc encryption software (Pointsec) was installed on the computer. The VPN certificate allowing remote access has been revoked. The Blackberry is similarly protected using encryption and a password screen lock. This case may be updated if further information becomes available.

Method of detection:
Visual

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:
Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
VPN certificate for laptop has been revoked. "Kill pill" will be sent to Blackberry.

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☒ Other Agencies (please specify) **Local (Seattle) law enforcement.**

Report Information (Call Center Use Only)

Report Date: 3/2/2012	**Report Time: 12:09 pm ET**

OFFICIAL USE ONLY

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 676031** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** March 6, 2012
Time incident *occurred*:	**Time incident *discovered*:** 8:50 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA SecurID webmail token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
On March 6, 2012 at 8:50 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.
We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)	
Report Date: 3/6/2012	**Report Time: 12:58 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 676044** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** March 6, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:05 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
On March 6, 2012 at 11:05 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 3/6/2012	**Report Time: 2:38 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information

Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 676073** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov

Incident Information

Date incident *occurred*:	**Date incident *discovered*:** March 6, 2012
Time incident *occurred*:	**Time incident *discovered*:** 2:15 p.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (RSA Token)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity: ☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	**Security Category:** ☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:
On March 6, 2012 at 2:15 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.
We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information

Who has been notified?
☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)

Report Information (Call Center Use Only)

Report Date: 3/6/2012	**Report Time: 6:17 pm ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 676074** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: (503) 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** March 6, 2012
Time incident *occurred*:	**Time incident *discovered*:** 2:35 p.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On March 6, 2012 at approximately 2:35 p.m. PST, the Office of Cyber Security received a report of a missing/lost Blackberry smartphone. The appropriate staff has been notified and the phone service has been terminated.

There was no known PII or SUI information on the device.

This case will be updated as further information becomes available.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
Kill pill was sent to the device. Service has been terminated.

Other Information

Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/6/2012	**Report Time: 6:31 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3-CIRC Ticket #: 676793 (Closed)** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):** PMA
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** March 15, 2012
Time incident *occurred*:	**Time incident *discovered*:** 3:40 p.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☒ RSA SecurID token
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☒ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected: N/A	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On March 15, 2012 at 3:40 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date: 3/15/2012	**Report Time: 7:29 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 677589** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** March 26, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:05 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On March 26, 2012 at 11:05 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:3/26/2012	**Report Time:2:45 PM ET**

U.S. Department of Energy
Office of the Chief Information Officer, Office of Cyber Security
(JC3) Joint Cybersecurity Coordination Center Incident Report
Incident type information: http://circ.jc3.doe.gov/incidentreporting.html

Contact Information	
Site Name: Bonneville Power Administration	**For Call Center use only:** **JC3 Ticket #: 677592** **OTHER Ticket #:** **US-CERT Ticket #:**
Contact name: April McCann	**Program Office Name (NNSA, SC, EM, etc.):**
Phone #: 503 230-5467	**Email address:** aamccann@bpa.gov
Incident Information	
Date incident *occurred*:	**Date incident *discovered*:** March 26, 2012
Time incident *occurred*:	**Time incident *discovered*:** 11:10 a.m., PST

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

IP Category:
☐ IP - ☐ PF - ☐ PS - ☐ PPM -
IP = Information Protection Incidents
PF = Protective Force/Executive Protection Incidents
PS = Physical Security Incidents
PPM = Program Planning and Management Incidents
Reference: IP Categories and Types https://aware.jc3.doe.gov/node/30

Information sensitivity:	**Security Category:**
☐ OUO ☐ PII ☐ SUI ☐ UCNI ☐ Other (please specify)	☐ Low Security Category: *limited* adverse affect ☐ Moderate Security Category: *serious* adverse affect ☐ High Security Category: *severe or catastrophic* adverse affect
# Machines affected:	**Which critical infrastructure was affected, if any?**
For Lost or Stolen Equipment: Was the drive(s) or file(s) Encrypted? Was the drive(s) or file(s) password protected? Other (please specify)	**For PII Incidents:** Number of individuals affected? Have the individuals been notified? Was the PII of Contractors or Federal employees?
IP address of affected machine(s):	**Operating system(s) of affected machine(s):**

Description of incident:

On March 26, 2012 at 11:10 a.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

Method of detection:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):**
Suspected method of intrusion/attack:	
Suspected perpetrators and/or possible motivations:	
Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

Impact and Actions Taken

Assessment of the impact of the incident:

What actions have been taken:
RSA Webmail Token has been disabled

Other Information	
Who has been notified? ☐ OIG ☐ FBI ☐ CI ☐ Other Agencies (please specify)	
Report Information (Call Center Use Only)	
Report Date:3/26/2012	**Report Time: 2:58PM ET**

From: McCann,April A (BPA) - NJB-B1
Sent: Thursday, June 21, 2012 1:25 PM
To: 'JC3'
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry,Sean P (BPA) - NJB-B1
Subject: INCIDENT REPORT - Missing/Lost RSA SecurID Webmail Token

Type 1 Incident / Security Category - Low

On June 21, 2012 at approximately 12:35 p.m. PST, the BPA Office of Cyber Security received a report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified and the webmail token has been disabled.

We do not anticipate any updates to this case and it can be closed.

April McCann

April A. D. McCann, NJB-B1
IT Specialist, Cyber Security
Bonneville Power Administration (BPA) - U.S. DOE
503.230-5467 / aamccann@bpa.gov
Cyber Security Main number - 503.230-5200
Cyber Security Emergency number - 503.230-5088

From: McCann,April A (BPA) - NJB-B1
Sent: Monday, May 21, 2012 2:05 PM
To: 'JC3'
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry,Sean P (BPA) - NJB-B1
Subject: RE: JC3-682799 - INCIDENT REPORT - Lost Laptop Computer

Hello,
The laptop computer has been found. Please close this ticket.
Thank you,
April
April A. D. McCann, NJB-B1
IT Specialist, Cyber Security
Bonneville Power Administration (BPA) - U.S. DOE
503.230-5467 / aamccann@bpa.gov
Cyber Security Main number - 503.230-5200
Cyber Security Emergency number - 503.230-5088

From: JC3 [mailto:circ@jc3.doe.gov]
Sent: Monday, May 21, 2012 10:31 AM
To: McCann,April A (BPA) - NJB-B1
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry,Sean P (BPA) - NJB-B1; JC3
Subject: JC3-682799 - INCIDENT REPORT - Lost Laptop Computer
To Whom It May Concern,

The attached information was reported to JC3 on 5/21/2012 at 1:21 PM ET. The JC3 has assigned ticket number JC3-682799 to this Incident. Please reference this ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

Robert Knisely
U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3-Call Center
1-866-941-2472
circ@jc3.doe.gov

From: McCann,April A (BPA) - NJB-B1 [mailto:aamccann@bpa.gov]
Sent: Monday, May 21, 2012 1:21 PM
To: JC3
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry, Sean
Subject: INCIDENT REPORT - Lost Laptop Computer

Type 1 Incident / Security Category - Low
On May 21, 2012 at 10:15 a.m. PST, the BPA Office of Cyber Security received a report of a lost laptop computer.

There was no known PII or SUI information on the computer. Encryption software was installed on the computer equipment - Pointsec. The VPN certificate allowing remote access has been revoked.
This case will be updated as further information becomes available.

April A. D. McCann, NJB-B1
IT Specialist, Cyber Security
Bonneville Power Administration (BPA) - U.S. DOE
503.230-5467 / aamccann@bpa.gov
Cyber Security Main number - 503.230-5200
Cyber Security Emergency number - 503.230-5088

From: JC3 <circ@jc3.doe.gov>
Sent: Tuesday, September 04, 2012 3:39 PM
To: McCann,April A (BPA) - NJB-B1; doecirc@doecirc.energy.gov; Gray, Whitney (CONTR); Hill, Ronald (CONTR); Kiehl, Brian (CONTR); Knisely, Robert (CONTR); Lertora, James (CONTR); Lim, Jesse (CONTR); Tankin Sr, Robert (CONTR); Ali, Minkah (CONTR)
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry,Sean P (BPA) - NJB-B1; JC3
Subject: RE: JC3-690916: INCIDENT REPORT - Missing/Lost Blackberry Smart phone

To Whom It May Concern,

The attached information was reported to JC3 on 9/4/2012 at 2:20 pm ET. The JC3 has assigned ticket number JC3-690916 to this Incident. Please reference this ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

RE: This ticket has been closed as requested

Manuel Luna
U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3 Call Center
1-866-941-2472
circ@jc3.doe.gov

From: McCann,April A (BPA) - NJB-B1 [mailto:aamccann@bpa.gov]
Sent: Tuesday, September 04, 2012 6:36 PM
To: JC3; doecirc@doecirc.energy.gov; Gray, Whitney (CONTR); Hill, Ronald (CONTR); Kiehl, Brian (CONTR); Knisely, Robert (CONTR); Lertora, James (CONTR); Lim, Jesse (CONTR); Luna, Manuel (CONTR); Tankin Sr, Robert (CONTR); Ali, Minkah (CONTR)
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry, Sean
Subject: RE: JC3-690916: INCIDENT REPORT - Missing/Lost Blackberry Smart phone

Hello,
No additional information. Please close this ticket.
Thank you,
April

April A. D. McCann, NJB-B1
IT Specialist, Cyber Security
Bonneville Power Administration (BPA) - U.S. DOE
503.230-5467 / aamccann@bpa.gov
Cyber Security Main number - 503.230-5200
Cyber Security Emergency number - 503.230-5088

From: JC3 [mailto:circ@jc3.doe.gov]
Sent: Tuesday, September 04, 2012 12:27 PM
To: McCann,April A (BPA) - NJB-B1; doecirc@doecirc.energy.gov; Gray, Whitney (CONTR); Hill, Ronald (CONTR); Kiehl, Brian (CONTR); Knisely, Robert (CONTR); Lertora, James (CONTR); Lim, Jesse (CONTR); Luna, Manuel (CONTR); Mandeville, John (CONTR); Tankin Sr, Robert (CONTR); Ali, Minkah (CONTR)

Subject: JC3-690916: INCIDENT REPORT - Missing/Lost Blackberry Smart phone
To Whom It May Concern,

The attached information was reported to JC3 on 9/4/2012 at 2:20 pm ET. The JC3 has assigned ticket number JC3-690916 to this Incident. Please reference this ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

Minkah Ali
U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3-Call Center
1-866-941-2472
circ@jc3.doe.gov

From: Blom,Aaron E (CONTR) - NJRH-2 [mailto:aeblom@bpa.gov] On Behalf Of Help Desk
Sent: Tuesday, September 04, 2012 2:20 PM
To: JC3
Cc: Cyber Security; Help Desk
Subject: INCIDENT REPORT - Missing/Lost Blackberry Smart phone

Type 1 Incident / Security Category - Low
On 9/4/2012 at approximately 10:43am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

From: JC3 <circ@jc3.doe.gov>
Sent: Wednesday, September 05, 2012 7:31 PM
To: Cyber Security; Help Desk
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry,Sean P (BPA) - NJB-B1; JC3
Subject: RE: JC3-691033: INCIDENT REPORT - Missing/Lost Blackberry Smart phone

To Whom It May Concern,

The attached information was reported to JC3 on 9/5/2012 at 4:01 pm ET. The JC3 has assigned ticket number JC3-691033 to this Incident. Please reference this ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

RE: This ticket has been closed as requested.

Thank you,

Manuel Luna
U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3 Call Center
1-866-941-2472
circ@jc3.doe.gov

From: Cyber Security [mailto:cybersecurity@bpa.gov]
Sent: Wednesday, September 05, 2012 10:28 PM
To: JC3; Help Desk
Cc: Cyber Security; Prouse,Gary L (BPA) - NJB-B1; Barry, Sean
Subject: RE: JC3-691033: INCIDENT REPORT - Missing/Lost Blackberry Smart phone

Hello,
No additional information. Please close this ticket.
Thank you,
April

April A. D. McCann, NJB-B1
IT Specialist, Cyber Security
Bonneville Power Administration (BPA) - U.S. DOE
503.230-5467 / aamccann@bpa.gov
Cyber Security Main number - 503.230-5200
Cyber Security Emergency number - 503.230-5088

From: JC3 [mailto:circ@jc3.doe.gov]
Sent: Wednesday, September 05, 2012 1:23 PM
To: Help Desk
Cc: Cyber Security; JC3
Subject: JC3-691033: INCIDENT REPORT - Missing/Lost Blackberry Smart phone
To Whom It May Concern,

The attached information was reported to JC3 on 9/5/2012 at 4:01 pm ET. The JC3

has assigned ticket number JC3-691033 to this Incident. Please reference this ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

Manuel Luna
U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3 Call Center
1-866-941-2472
circ@jc3.doe.gov

From: Blom,Aaron E (CONTR) - NJRH-2 [mailto:aeblom@bpa.gov] On Behalf Of Help Desk
Sent: Wednesday, September 05, 2012 4:01 PM
To: JC3
Cc: Cyber Security; Help Desk
Subject: INCIDENT REPORT - Missing/Lost Blackberry Smart phone

Type 1 Incident / Security Category - Low
On 9/5/2012 at approximately 12:54pm PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.

From: McCann,April A (BPA) - NJB-B1
Sent: Monday, September 10, 2012 3:32 PM
To: 'JC3'
Cc: Howard,Lance (BPA) - NJB-B1; Prouse,Gary L (BPA) - NJB-B1;
Barry,Sean P (BPA) - NJB-B1
Subject: RE: JC3-691483 - INCIDENT REPORT - Missing/Lost RSA SecurID
Webmail Token (open/closed)

Hello,
No additional information. Please close this ticket.
Thank you,
April

April A. D. McCann, NJB-B1
IT Specialist, Cyber Security
Bonneville Power Administration (BPA) - U.S. DOE
503.230-5467 / aamccann@bpa.gov
Cyber Security Main number - 503.230-5200
Cyber Security Emergency number - 503.230-5088

From: JC3 [mailto:circ@jc3.doe.gov]
Sent: Monday, September 10, 2012 2:30 PM
To: Howard,Lance (BPA) - NJB-B1; McCann,April A (BPA) - NJB-B1
Cc: JC3
Subject: JC3-691483 - INCIDENT REPORT - Missing/Lost RSA SecurID Webmail Token (open/closed)
To Whom It May Concern,

The attached information was reported to JC3 on 9/10/2012 at 4:37 PM ET. The JC3 has assigned ticket number JC3- 691483 to this Incident. Please reference this ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

RE: Unable to send entrusted email to Derek Sutro, Help Desk, Cyber Security or Server Access Control - NJNI-2

Ron Hill
U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3 Call Center
1-866-941-2472
circ@jc3.doe.gov

From: Sutro,Derek S (CONTR) - NJRH-2 [mailto:dssutro@bpa.gov] On Behalf Of Help Desk
Sent: Monday, September 10, 2012 4:37 PM
To: JC3
Cc: Cyber Security; Server Access Control - NJNI-2; Help Desk
Subject: INCIDENT REPORT - Missing/Lost RSA SecurID Webmail Token

Type 1 Incident / Security Category - Low

On [Date 09-10-2012] at approximately 1:20PM PST, the BPA Help Desk received a

report of a missing/lost RSA SecurID webmail token. The appropriate staff has been notified to disable the webmail token.

We do not anticipate any updates to this case and it can be closed.

From: JC3 <circ@jc3.doe.gov>
Sent: Tuesday, September 11, 2012 12:38 PM
To: McCann,April A (BPA) - NJB-B1; Howard,Lance (BPA) - NJB-B1
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry,Sean P (BPA) - NJB-B1; JC3
Subject: RE: JC3-691568 - INCIDENT REPORT - Missing/Lost Blackberry Smart phone

To Whom It May Concern,

The attached information was reported to JC3 on 9/11/2012 at 12:09 PM ET. The JC3 has assigned ticket number JC3-691568 to this Incident. Please reference this ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

RE: The ticket has been closed as requested.

Thank you,

Manuel Luna
U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3 Call Center
1-866-941-2472
circ@jc3.doe.gov

From: McCann,April A (BPA) - NJB-B1 [mailto:aamccann@bpa.gov]
Sent: Tuesday, September 11, 2012 3:36 PM
To: JC3; Howard,Lance (BPA) - NJB-B1
Cc: Prouse,Gary L (BPA) - NJB-B1; Barry, Sean
Subject: RE: JC3-691568 - INCIDENT REPORT - Missing/Lost Blackberry Smart phone

Hello,
No additional information. Please close this ticket.
Thank you,
April
April A. D. McCann, NJB-B1
IT Specialist, Cyber Security
Bonneville Power Administration (BPA) - U.S. DOE
503.230-5467 / aamccann@bpa.gov
Cyber Security Main number - 503.230-5200
Cyber Security Emergency number - 503.230-5088

From: JC3 [mailto:circ@jc3.doe.gov]
Sent: Tuesday, September 11, 2012 9:49 AM
To: Howard,Lance (BPA) - NJB-B1; McCann,April A (BPA) - NJB-B1
Cc: JC3
Subject: JC3-691568 - INCIDENT REPORT - Missing/Lost Blackberry Smart phone
To Whom It May Concern,

The attached information was reported to JC3 on 9/11/2012 at 12:09 PM ET. The JC3 has assigned ticket number JC3-691568 to this Incident. Please reference this

ticket number when contacting the JC3 Call Center with questions or updated information. You can contact the JC3 by phone at 1-866-941-2472 or send an email to circ@jc3.doe.gov.

RE: Corrected subject line with proper ticket number

Ron Hill
U.S. Department of Energy
Joint Cybersecurity Coordination Center (JC3)
Contractor supporting Office of the CIO
JC3 Call Center
1-866-941-2472
circ@jc3.doe.gov

From: Blom,Aaron E (CONTR) - NJRH-2 [mailto:aeblom@bpa.gov] On Behalf Of Help Desk
Sent: Tuesday, September 11, 2012 12:09 PM
To: JC3
Cc: Cyber Security; Help Desk
Subject: INCIDENT REPORT - Missing/Lost Blackberry Smart phone

Type 1 Incident / Security Category - Low
On 9/11/2012 at approximately 8:57am PST, the BPA Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service.

There was no known PII or SUI information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. BPA does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

This case will be updated as further information becomes available.