



## Department of Energy

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

PUBLIC AFFAIRS

March 1, 2013

In reply refer to: DK-7

Jehan Patterson  
1600 20<sup>th</sup> Street, NW  
Washington, DC 20585

### FOIA #BPA-2013-00497-F

Dear Mr. Patterson:

This is a final release in response to your request for records that you made to the Bonneville Power Administration (BPA), under the Freedom of Information Act (FOIA), 5 U.S.C. 552.

#### **You requested the following:**

(1) all contracts or agreements, including but not limited to any sub-contracts or sub agreements, between the Department of Energy ("DOE") and third-party vendors that provide security for all DOE computer networks ("third-party security vendors"), including but not limited to any networks that are accessible only to DOE employees and staff and any networks accessible to members of the public;

**Response:** BPA does not have any contracts, agreements, sub-contracts or sub-agreements with third-party vendors that provide security for all DOE/BPA computer networks. This has been confirmed through BPA's Supply Chain, A&E Supplemental Labor and IT Contracting, IT Spend Manager. BPA's Network Services concurred.

(2) all records that constitute or concern DOE's policies, protocols, or guidance regarding the selection and/or creation of filters to block access to websites on any DOE computer network;

(3) all records that constitute or concern DOE's policies, protocols, or guidance regarding the designation of websites to which filters blocking access are or have been applied, including but not limited to filter(s) concerning political or activist groups, on any DOE computer network;

(4) all records that constitute or concern DOE's policies, protocols, or guidance regarding the review and/or removal of filters that are or have been applied to websites on any DOE computer network;

**Response:** BPA has released the following files on the enclosed CD and they are released in their entirety:

- BPAM 1115 (PCSP) Appendix A- Identification, Authentication and Access Control Program v1.pdf
- BPAM 1140 Use of Social Media.pdf
- BPAM 1110.pdf

(5) all records that concern or refer to websites to which filter(s) concerning political or activist groups are or have been applied on any DOE computer network;

(6) all records regarding DOE's application, and/or removal of filters of websites, including but not limited to filter(s) concerning political or activist groups, on any DOE computer network;

**Response:** BPA has released the following files on the enclosed CD:

- BPA-2013-00497-FRequest Firewall Block Rules-redacted.pdf
- SurfControlBlackList-redacted.pdf
- SC to Websense Xwalk.pdf
- Cyber Security FOIA SMTP.pdf

BPA has withheld some information on these files under Exemption 6 of the FOIA. BPA asserts this exemption for information which could reasonably be expected to constitute an unwarranted invasion of personal privacy if disclosed. The withheld information consists of the names and locations of individual employees. Release of this information could subject these individuals to unwanted intrusions of privacy. There is no public interest in the disclosure of this information because it does not shed any light on how BPA has performed its statutory duties.

(7) all records that constitute or memorialize communications among DOE and third-party security vendors regarding filters applied to websites on any DOE computer network, including but not limited to communications regarding implementation of DOE policies, protocols, or guidance concerning filter(s) of political or activist group websites

**Response:** BPA has no responsive records.

(8) all records that constitute or memorialize communications among DOE and third-party security vendors regarding removal of filter(s), including but not limited to filter(s) concerning political or activist groups, on any DOE computer network;

**Response:** BPA has no responsive records.

(9) all records that constitute or memorialize communications between DOE and any DOE employee who has requested access to, and/or DOE review of, website(s) that is or have been filtered on any DOE computer network;

(10) all records that constitute or memorialize communications between DOE and non-DOE individuals or groups requesting access to, and/or DOE review of, website(s) that are or have been filtered on any DOE computer network.

**Response:** BPA has released the following files on the enclosed CD:

- CRMwebsiteunblocked-redacted.pdf
- CRMwebsiteblocked-redacted.pdf

BPA has withheld some information on these files under Exemption 6 of the FOIA. Please see above for an explanation of Exemption 6.

Pursuant to 10 CFR 1004.8, if you are dissatisfied with this determination, or the adequacy of the search, you may appeal this FOIA response in writing within 30 calendar days of receipt of a final response letter. The appeal should be made to the Director, Office of Hearings and Appeals, HG-1, Department of Energy, 1000 Independence Avenue, SW, Washington, DC 20585-1615. The written appeal, including the envelope, must clearly indicate that a FOIA Appeal is being made.

I appreciate the opportunity to assist you. Please contact Kim Winn, FOIA Specialist, at 503-230-5273 with any questions about this letter.

Sincerely,

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

Enclosure: CD



**U. S. Department of Energy**  
**Bonneville Power Administration**  
**Office of the Chief Technical Officer**  
**Identification, Authentication and Access Controls**



- I. SUBJECT:** This document establishes the Bonneville Power Administration’s (BPA) formal access control policy. Access to BPA information resources will be limited to personnel, systems and processes needing the resources to perform assigned duties. The principles of separation of duties and least privilege will be applied to the allocation of access rights.
- II. SCOPE:** This policy and related standards applies to all internal BPA information users, owners and custodians. Systems designated as being part of the bulk electric system and subject to compliance with the provisions of National Electric Reliability Council Critical Infrastructure Protection standards pursuant to the Energy Policy Act of 2005 (Pub. L. 109-58) must comply with both these standards and the provisions of the Grid Operations Information System Security Manual.
- III. DESCRIPTION:** Access control capabilities provide the agency a standard mechanism to manage and control entities utilizing BPA information systems. The goal of access control is to protect an organization’s resources from unauthorized access while facilitating seamless and legitimate use of these resources. As a federal agency, BPA is required to adhere to these practices, including the implementation of guidelines from the National Institute of Standards and Technology (NIST), pursuant to the Federal Information Security Management Act (FISMA). This document addresses controls from NISTSP 800-53, Revision 3 control families Access Control (AC) and Identification and Authentication (IA). Requirements from the Department of Energy Cyber Security Program (as established in DOE Order 205.1B), and in some cases North American Electric Reliability Corporation (NERC) standards and requirements from the Committee on National Security Systems (CNSS), also apply to access control policies and procedures.
- IV. POLICY:** Identification and authentication access controls shall be provided for all personnel, devices and processes requiring access to information systems supporting agency mission and functions and/or deployed on behalf of the agency. This access shall be commensurate with each information system’s security category (based on FIPS 199), as well as the principles of least access (limiting access to only necessary information to perform assigned duties) and separation of duties (preventing error or fraud by requiring two or more individuals to coordinate tasks). This policy shall be enacted by adhering to the Procedures and Standards described in Section V.
- V. PROCEDURES & STANDARDS:** The following standards and procedures shall be implemented for all information systems operated by, on behalf of, BPA.



---

These policies and standards require written approval and documentation for each known and granted exception to these policies and standards.

A. Account Management (AC-2)

- Each standard (non-privileged) user account will be uniquely identified. (AC-2a, IA-2)
- Each extended (privileged) user account will be uniquely identified in a manner which clearly distinguishes the privileged account from standard, service and guest/temporary accounts. (AC-2a, IA-2, IA-4b)
- Each extended (privileged) user account will ONLY be utilized for purposes of performing administrative tasks on the information system or systems. Other activities must be avoided to prevent malicious code and similar activity from impacting system operations. (NERC-CIP-007-3 R5.2)
- Each service account will be uniquely identified in a manner which clearly distinguishes the service account from standard, privileged and guest/temporary accounts. (AC-2a, IA-2, IA-4b)
- Each shared account will be uniquely identified in a manner which clearly distinguishes the shared account from standard, privileged and guest/temporary accounts. (AC-2a, IA-2, IA-4b)
- Each guest/temporary account will be uniquely identified in a manner which clearly distinguishes the guest/temporary account from standard, privileged and service accounts. (AC-2a, AC-2f, IA-2, IA-4b)
- All activity of each guest/temporary account will be audited and monitored while active and in-use. (AC-2f)
- Each guest/temporary account will be uniquely identified in a manner which clearly distinguishes the guest/temporary account from standard, privileged and service accounts. (AC-2a, AC-2f, IA-2, IA-4b)
- All activity of each guest/temporary account will be audited and monitored while active and in-use. (AC-2f)
- All individuals with access to a shared account will be documented by the Information System Owner (ISO). (NERC-CIP-3 R5.2.2)
- For each system, the ISO will define access rights and privileges for system users based on the business requirements for access defined by the Information Owner (IO) and assign user access to the system to ensure each user has the minimum necessary access (Least Privilege) necessary to perform their job function. (AC-2b, AC-2c, AC-2i, AC-6, NERC-CIP-007-3 R5.1, NERC-CIP-007-3 R5.1.1)
- For each account, the ISO will authorize access to information systems for individual standard user accounts, extended (privileged accounts), service accounts and temporary accounts prior to these accounts connecting to the information system. (AC-2d, AC-2e, IA-4a)



- 
- A unique user identifier will be established for a user once authorization to create a specific type of account (non-privileged, privileged, service or guest/temporary) is approved for creation by (list of defined authorizers) (AC-2d, AC-2e, IA-2, IA-4a, IA-4b)
  - All accounts on all Information Systems will be reviewed and audited regularly (at least every 90 days for FIPS199 rated HIGH systems, every 6 months for MODERATE systems and every year for LOW systems) by the respective ISO to ensure the correct users are the granted access and incorrect user accounts and/or access privileges are removed. (AC-2e, AC-2j, NERC-CIP-003-3 R5.2, NERC-CIP-004-3 R4.1, NERC-CIP-007-3, R5.1.3)
  - Unique user identifiers will not be reused within one year of the last usage date. (AC-2e, IA-4d)
  - Disabled computer accounts will be automatically deleted and removed from the system after 60 days of inactivity. (AC-2e, AC-2 Enhancement 1, AC-2 Enhancement 2)
  - Approved and authorized Non-Organizational users requiring access to BPA organizational assets located inside the BPA internal environment will be granted guest accounts with specific termination dates. Access must be approved by an X level Bonneville full-time employee. (AC-2f, AC-2i, IA-8)
  - ISO's, or their designated representative, will be notified when guest/temporary accounts are no longer needed and when employees (permanent and contract) are terminated, transferred, or information system access is no longer required. (AC-2g)
  - The password for Shared accounts will be changed immediately in the event of personnel changes (transfer, change in responsibilities, or termination). (NERC-CIP-3 R5.2.3)
  - Temporary user accounts shall be automatically disabled after 60 days and require explicit reauthorization by the ISO prior to re-enabling these accounts. (AC-2h, AC-2 Enhancement 1, AC-2 Enhancement 2)
  - User accounts of terminated employees will be disabled within 24 hours of the actual termination date as indicated on the Final Pay Clearance by Server Access Control. (AC-2h)
  - BPA uses a single, standard enterprise directory model to manage enterprise access and resources. Systems, services and applications supporting BPA must integrate into this environment for purposes of user access management. (AC-2 Enhancement 1, AC-3)
  - BPA will use user authentication protocols which are compatible with Active Directory and are resistant to replay style attacks. (AC-2 Enhancement 1)
  - Unused computer accounts will be automatically disabled after 30 days of inactivity. (AC-2 Enhancement 1, AC-2, Enhancement 3, IA-4e)



B. Access Enforcement (AC-3)

C. Information Flow Enforcement (AC-4)

- All Information Systems will be deployed into established computing environments which control access to systems from potentially hostile networks through the use of firewalls, proxy servers and access control lists. (AC-4)

D. Separation of Duties (AC-5)

- Access rights within a system will be configured so certain key tasks (e.g., creating and signing a check) are separated and require different users with different access accounts to create and approve the transaction. (AC-5.a, NERC-CIP-007-3 R5.1)
- Access rights within a system will be documented (e.g. rights matrix) in such as way as to ensure separation of duties. (AC-5b)

E. Least Privilege (AC-6)

- All accesses to security functions and/or security related information will be explicitly authorized by the ISO (AC-6, Enhancement 1)
- A standard user account will not be granted access to administrative functions. (AC-6, Enhancement 2)

F. Unsuccessful Login Attempts (AC-7)

- Accounts entering incorrect passwords 3 consecutive times will be disabled, requiring manual resetting of the account before access can be achieved. (AC-7a, AC-7b)

G. System Use Notification (AC-8)

- All Information systems will display an approved system use notification message before or during the login process and prior to allowing access to data on the information system. (AC-8a, AC-8b, AC-8c)
- Do we want to include the specific language used for domain logon and others (external users?)

H. Concurrent Session Control (AC-10)

- The information system will limit the number of sessions for any single account to 1. (AC-10)



#### I. Session Lock (AC-11)

- All Information system sessions will be locked (requiring re-authentication) after 5 minutes of inactivity. All information system sessions will be terminated after 15 minutes of inactivity. The session lock will remain in effect until the session is reestablished using established identification and authentication procedures. (AC-11a, AC-11b)

#### J. Permitted Actions without Identification or Authentication (AC-14)

- No actions will be performed on any information system until the user has been identified and authenticated using established procedures. (AC-14a, AC-14b, AC-14 Enhancement 1)

#### K. Remote Access (AC-17)

- Remote access to specific client devices by BPA staff for non-privileged access requires two-factor authentication. (AC-17a, AC-17 Enhancement 7, IA-2 Enhancement 2)
- Remote access to specific administrative systems by BPA staff for privileged access requires two-factor authentication. (AC-17a, AC-17 Enhancement 7, IA-2 Enhancement 1)
- Remote access to web-based electronic mail via the Internet requires two-factor authentication. (AC-17a, AC-17 Enhancement 7)
- Remote access to internal network services will authenticate through at least two-factor authentication methods (e.g., tokens, PKI). (AC-17a, AC-17 Enhancement 2, AC-17 Enhancement 7, IA-2 Enhancement 8, IA-2 Enhancement 9)

#### L. Wireless Access (AC-18)

- Wireless access points will not directly connect to the BPA internal network. (AC-18a)
- General wireless access to general BPA resources (e.g., supporting broad usage such as connecting to email, web, and similar BPA resources) will be provided using existing systems, services and technologies supporting remote access. (AC-18a, AC-18 Enhancement 1, AC-18 Enhancement 4)

#### M. Access Control for Mobile Devices (AC-19)

- Portable and mobile devices (e.g., laptop computers, cellular telephones, tablet computers, e-book readers, etc.) connecting to the BPA network and/or access BPA resources will be locally encrypted and password protected following the appropriate standards in this document. (AC-19a)



- 
- All BPA-owned mobile devices will be scanned, by BPA-approved methodologies, when returning from locations of significant risk, as determined by BPA. (AC-19g)
  - Only BPA owned and issued removable media will be connected to any BPA information system. (AC-19 Enhancement 1, AC-19 enhancement 2, AC-19 Enhancement 3)

#### N. Use of External Information Systems (AC-20)

- Prior to authorizing access to any BPA information system from an external system, the ISO must ensure the required security controls on the external system are implemented and meet, or exceed, those required for the BPA information system. (AC-20a, AC-20b, AC-20 Enhancement 1, AC-20 Enhancement2)

#### O. Identification and Authentication of Organizational Users (IA-2)

- Local access to specific client devices by BPA staff for non-privileged access requires single-factor authentication. (IA-2 Enhancement 4 requires multifactor)
- Local access to specific administrative systems by BPA staff for privileged access requires two-factor authentication. (IA-2 Enhancement 3)

#### P. Identification and Authentication of Devices (IA-3)

- Each client, server and storage device attached to the network will have a unique IP address assigned through DHCP services. Network devices with static addresses shall be assigned through static device configuration. (IA-3, IA-4c)

#### Q. Identifier Management (IA-4)

- Devices requiring static addresses will document the assignment of the IP addresses through a permanent DHCP reservation to prevent accidental reuse. (IA-4c)
- Devices with static DHCP address will be assigned a permanent name in DNS. (IA-4c)

#### R. Authenticator Management (IA-5)

- All default passwords will be changed upon installation of the information system or software. (IA-5e)



- 
- Prior to issuing the initial authenticator (user account and password), the issuing authority must verify the identity of the individual receiving the information and verify the individual is authorized to receive the information. (IA-5a)
  - All passwords used to access BPA resources will be no less than 8 characters in length. [PIN numbers utilized as part of two-factor authentication shall not be subject to this restriction.] (IA-5c, NERC-CIP-007-3 R5.3.1)
  - All passwords used to access BPA resources will consist of at least one character each of three of the four following key-space elements (upper case, lower case, number and symbols). [PIN numbers utilized as part of two-factor authentication shall not be subject to this restriction.] (IA-5c, IA-5 Enhancement 1a, NERC-CIP-007-3 R5.3.2)
  - Passwords will be required to be different than the last 6 passwords used for the information system. (IA-5c, IA-5 Enhancement 1e)
  - All password systems will be configured to only allow passwords to be changed once every 24 hours. (IA-5f, IA-5 Enhancement 1d)
  - All passwords used to access BPA resources will be changed at least once every 60 days for interactive user accounts, and at least once every 180 days for system and service accounts. (IA-5f, IA-5g, IA-5 Enhancement 1d, NERC-CIP-007-3 R5.3.3)
  - All passwords will be encrypted both at rest and in transmission. (IA-5h, IA-5i, IA-5 Enhancement 1c)
  - Passwords displayed in interactive login sessions (when a human logs on to a system) will be obscured from being read by displaying asterisks, dots, bubbles or other markers in place of the actual password. (IA-5h, IA-5i, IA-6)
  - All password systems will be configured to only allow passwords to be changed by an Information System administrator or by the user to whom the password is associated to. (IA-5i)
  - All passwords used to access BPA resources will change a minimum of 4 characters each time they are changed. (IA-5 Enhancement 1b)

#### S. Cryptographic Module Authentication (IA-7)

BPA will utilize FIPS 140-2 certified cryptographic modules for encryption services. (IA-7).



---

## V. ROLES AND RESPONSIBILITIES:

Teams and individual roles involved in access control can include the following:

- A. **Information Owners (IO)** - Official with statutory or operational authority for specified information (data). The Information Owner is the primary custodian of business data within an information system and responsible for defining the types of data within the system and the impact of disruption to this data based on the Agency-Level Consequence Scales.
- B. **Information System Owners (ISO)** - The Information System Owner is responsible for defining specific security requirements and practices for a system based on the business requirements of the system as set by the Information Owner across the entire lifecycle of the Information System and in compliance with these security standards. Responsible for ensuring remediation efforts to correct control deficiencies are resolved.
- C. **System Security Manager (SSM)** - System Security Managers are responsible for implementing and managing security controls for a given information system to meet the security requirements set for by the Information System Owner and in compliance with these security standards. Responsible for resolving remediation efforts to correct control deficiencies.
- D. **Chief Technical Officer (CTO)** - organizational official responsible for developing and maintaining information security policies, procedures and control techniques to address all applicable requirements on behalf of the CIO.
- E. **Chief Information Officer (CIO)** - organizational official responsible for designating a senior agency information security officer, who acting on behalf of the Agency will monitor organizational Information Systems for compliance to these security standards, provide reporting and assist in tracking remediation activities.

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 0;">Part: Information Management and Technology</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Page 1110-1</td> </tr> <tr> <td style="padding: 5px;">Date 01/03/07</td> </tr> </table>	Page 1110-1	Date 01/03/07
Page 1110-1				
Date 01/03/07				

### 1110.1 PURPOSE

To provide Cyber Security policy on the use of BPA Information Technology Services. This policy applies to all personnel who have authorized access to BPA facilities and sites, including BPA federal and contractor employees and visitors. This policy applies to all BPA IT Equipment as defined in Chapter 1110.

The misuse of BPA IT Equipment and Information Technology Services poses significant risks to mission and business of the BPA.

### 1110.2 DEFINITIONS

- A. Authorized Systems Users** are BPA federal and contractor employees who have (1) undergone and passed a background security screening in accordance with current federal requirements; (2) been issued physical access; (3) been issued a logon account to the Bonneville User Domain (BUD) administrative network and/or access to any other BPA computer system or network; and (4) taken the mandatory annual Security and Emergency Management and Cyber Security training and have been validated as completing that training.
- B. Blog** is short for **web Log**. A blog is a Web page that serves as a publicly accessible personal journal for an individual, group, or community, including businesses. Typically updated daily, blogs often reflect the personality of the author.
- C. Businesslike** is practical and unemotional, purposeful and earnest; exhibiting methodical and systematic characteristics that would be useful in business.
- D. BPA Authorized Installers** are designated personnel who are authorized to install, update and remove BPA licensed software on workstation (desktop or laptop) computing devices. In addition, BPA Authorized Installers are authorized to install, modify and move BPA IT Equipment.
- E. BPA Cyber Security** is the official organization responsible for development, issuance, and enforcement of policy relating to BPA IT Equipment. Cyber Security's governance is based on federal laws, regulations, DOE Orders and BPA guidelines. All Cyber Security policies and other materials can be found on the [Cyber Security Office web site](#).
- F. BPA federal employees** are employees and supervisors employed by the federal government and BPA.
- G. BPA's Harassment-Free Workplace Policy** is provided by BPA Manual Chapter 400/700A, Appendix A.
- H. BPA IT Equipment** includes BPA's computer networks and any authorized BPA-owned computing device or component that can be attached or connected to BPA's computer network. BPA IT Equipment includes desktop computers and monitors, laptop and portable computers, software, freeware, personal digital assistants (PDAs), telephones, digital cameras, cell phones, smart phones, facsimile machines, pagers, copiers, photocopiers, printers, scanners, servers, fixed or portable storage devices (flash drives), routers, peripheral devices and multi-purpose machines (combined facsimile, printer and copier).
- I. BPA IT Support Staff** are designated personnel who are authorized to support and modify certain settings on workstation (desktop or laptop) computing devices. They are reached by contacting the Help Desk.
- J. BPA Supervisors** are BPA federal employees whose position duties include performance and/or conduct supervision of other BPA federal employees.
- K. Broadcast e-mail** is the distribution of an e-mail message to a large group (50 or more) of BPA federal and contractor employees, rather than addressing the e-mail message to a limited number of specific, individually-named BPA employees or other recipients.



## Chapter 1110: Business Use of BPA Information Technology Services Policy

Part: Information Management and Technology

- L. **Chain e-mail** is the electronic equivalent of the chain letter which is a letter that explicitly directs the recipient to distribute copies of the letter to others.
- M. **Chat Room** is a web site, part of a web site, or part of an online service, that provides a venue for communities of users with a common interest to communicate in real time. Forums and discussion groups, in comparison, allow users to post messages but don't have the capacity for interactive messaging.
- N. **Configuration Settings** are persistent or saved values that describe operational parameters for software, including operating systems and hardware. Configuration settings are standardized at BPA and users are prohibited from changing those settings. For example, password changes are set for every ninety days as a standard configuration setting on the BPA administrative network.
- O. **Contractor** is defined by the Bonneville Purchasing Instructions (BPI) in part 1.8, page 1-5 as a firm or individual that currently has a contract to supply goods or services to BPA.
- P. **Contractor employee** is the employee of a contractor or is an independent contractor who has a contract with BPA to provide personnel to perform specific tasks. The contractor-BPA employee relationship is governed by the BPA contract and managed by the Contracting Officer (CO) and the Contracting Officer's Technical Representative (COTR).
- Q. **Contracting Officer (CO)** is the BPA official delegated to award binding contracts on behalf of BPA to contractors and who is responsible for appointing and Contracting Officer's Technical Representative (COTR) to administer the contract.
- R. **Contracting Officer's Technical Representative (COTR)** is appointed by the Contracting Officer by a delegation letter and administers the contract after it has been awarded. For the purposes of this Chapter, the COTR is the person who performs the day-to-day management of the contract.
- S. **Controlled Access Point** is a restricted communication boundary through which an authorized software connection can be made to a computer system on the other side.
- T. **Data** are the plural of datum and are distinct or discreet pieces of information usually formatted as data types (integer, string, etc.) and can exist electronically in database files, free text files, spreadsheet files. Data typically has no syntactical or grammatical meaning with regard to human use. Computers are capable of using such data.
- U. **Database** is a collection of information stored in a computer in a systematic way, such that a computer program can consult it to answer questions. The software used to manage and query a database is known as a database management system (DBMS).
- V. **Download** is the transfer of electronic files from a source to a destination. **Downloading** is the process of transferring electronic files from a source to a destination.
- W. **Dual Use IT Equipment** is IT Equipment that is used as both Administrative/General Purpose IT Equipment and Operational and Control IT Equipment and that may be authorized for access on the BUD administrative network with Cyber Security's authorization.
- X. **Electronic mail (e-mail)** is the exchange of computer-stored messages and attachments (files) across a network, which includes the Internet, using BPA-provided IT Equipment. The author of an e-mail message creates and sends (including forwarding of and/or replying to a received e-mail message) the e-mail message to one or more recipients by specifying the recipients' e-mail address. An e-mail author can also send a message to several recipients at once using a group e-mail address. Sent and received e-mail messages are stored in electronic mailboxes until retrieved by the e-mail user.



# BPA MANUAL

Page  
1110-3

## Chapter 1110: Business Use of BPA Information Technology Services Policy

Date  
01/03/07

Part: Information Management and Technology

- Y. File** is an electronic collection of binary digits (bits) and bytes (eight bits) typically characterized by a file name and an extension, although in some operating systems, a file extension is not mandatory. A file may contain text, images, motion pictures, binary data, delimited data, audio samples, Internet pages among others.
- Z. Financial Transaction** is an exchange or transfer of money from one account to another using BPA IT Equipment.
- AA. Freeware** may be commercial or non-commercial software that is available to the public at no charge. Often the licensing agreement does not contain terms acceptable to BPA. Freeware is high risk software that is typically not supported by a formal organization nor well tested or built on industry standards. It poses a significant risk to the BPA computing environment and is only permitted with Cyber Security approval. It may not be downloaded or installed without express approval.
- BB. Gambling** (gaming, betting) is to play at any game of chance for money or other stakes using BPA IT Equipment.
- CC. Guidance** is information that provides direction or advice as to a decision or course of action.
- DD. Improper Use** is that which meets the criteria of unsuitable, improper or inappropriate as defined in this Chapter and in additional Cyber Security and Employee Relations policies currently in force.
- EE. Incremental Charges** are financial charges levied on BPA that can be traced back to the specific usage incidence and the BPA federal and contractor employee responsible for incurring that charge. An example of such a charge would be calls made via cellular phone that are itemized on the monthly bill from the cell phone provider.
- FF. Information** is data that has been processed to add or create meaning for the person who receives it.
- GG. Information Technology (IT)** is any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
- HH. Internet (or Net or Web or World Wide Web)** is a global network connecting millions of computers in which users at any one computer can, if they have system permission, get information from any other computer (and sometimes communicate electronically directly to users at other computers). The interconnections between so many computers and computer users, makes the Internet a highly efficient tool for research and communication. It also poses significant vulnerability to Internet users from malicious software.
- II. IT Acquisition Review Board (ITARB)** - deleted 01-12-2007. The ITARB ceased functioning during the revision of this document.
- JJ. Non-work time** is defined as the time before an employee's workday begins, after the workday ends, or during lunch.
- KK. Operational and Control IT Equipment** is any standalone BPA IT Equipment dedicated full time for control of the BPA electrical system and is not authorized for access on the BUD administrative network without Cyber Security approval.
- LL. Password** is a confidential/secret string of characters (letters, numbers, and other symbols) used in conjunction with a user ID to authenticate an identity or to verify access authorization.
- MM. Personal Financial Transaction** is an exchange or transfer of funds (monies) on BPA Equipment to procure personal goods or services or to pay personal invoices or bills.

	<h1>BPA MANUAL</h1> <h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p>Part: Information Management and Technology</p>	Page 1110-4
		Date 01/03/07

**NN. Personal IT Equipment** is any non-BPA IT Equipment.

**OO. Personal Use** is use of BPA IT Equipment by BPA federal and/or contractor employees for non-BPA business and is defined by BPA Manual Chapter 1110A: Allowance for Limited Personal Use of BPA Information Technology Equipment.

**PP. Pornography** is pictures and/or writings of sexual activity intended solely to excite lascivious feelings, of a particularly blatant and aberrational kind such as acts involving children, animals, orgies, and all types of sexual intercourse.

**QQ. Posting** is publishing information, documents, images or audio in an online environment such as a web site, chat room, message board, blog.

**RR. Peripheral Devices** are computer devices, such as a DVD-ROM drive, flash drive or printer, that is not part of the essential computer, i.e., the memory and microprocessor. Peripheral devices can be external – such as a mouse, keyboard, printer, monitor, external hard drive or scanner – or internal, such as a DVD-ROM drive, DVD-R drive or internal modem. Internal peripheral devices are often referred to as integrated peripherals.

**SS. Personally Identifiable Information (PII)** is any information about an individual maintained by an agency, including, but not limited to education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. [Source: [Cyber Security Policy](#) BPA-20060809-001]

**TT. Presentation Settings** refer to the Microsoft Windows Screen Saver Display Properties menu which controls the appearance of the software on the display screen. Display Properties consist of settings for screen resolution and color depth, desktop background image (wallpaper), screen saver settings, configuration, and images, and appearance of windows and buttons.

**UU. The Privacy Act of 1974, 5 U.S.C. § 552a (2000)** is generally characterized as an omnibus “code of fair information practices” that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies.

**VV. Remote Access Service (RAS)** is the ability to gain authorized access to BPA IT Equipment through a controlled access point from locations outside the BPA work environment. Cisco's Virtual Private Network (VPN) is an example of software used to permit secure authorized access through a controlled access point.

**WW. Sensitive Unclassified Information (SUI)** includes unclassified information requiring protection mandated by policy or laws, such as Privacy Act Information, proprietary information, Export Control Information (ECI), Unclassified Controlled Nuclear Information (UCNI), and Personally Identifiable Information (PII). [Source: US-DOE: Protection of Sensitive Unclassified Information, Including Personally Identifiable Information, September 6, 2006.]

**XX. Shareware** is essentially non-commercial software created by independent software developers that is often free but sometimes requires users to pay a license fee. Often the licensing agreement does not contain terms acceptable to BPA. Shareware is also high risk software that is typically not supported by a formal organization and not well tested. It poses a significant risk to the BPA computing environment and is only permitted with Cyber Security approval. It may not be downloaded or installed without express approval.

**YY. Standards of Ethical Conduct for Government employees** are defined by 5 CFR § 2635.

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 0;">Part: Information Management and Technology</p>	<p style="margin: 0;">Page 1110-5</p> <hr/> <p style="margin: 0;">Date 01/03/07</p>
--	--	---

**ZZ. User** is any federal and/or contractor employee authorized to use BPA IT equipment.

**AAA. User ID (userid, user identification)** is one half of the authentication identifier assigned to authorized users that is required with the user’s password to access computer systems that require authentication.

**BBB. Weapon** is any instrument or instrumentality used defensively for fighting, combat, and hunting such as but not limited to a semi-automatic or automatic gun (hand gun, pistol, revolver, rifle, etc.), ammunition, gun parts, sword, knife, missile, spear, bomb, explosive chemicals or parts or incendiaries.

### 1110.3 POLICY

This policy is promulgated under the authority of Title III – Information Security, Federal Information Security Management Act of 2002, Chapter 35 of Title 44, United States Code, § 3544. Federal agency responsibilities A.3.(C) “developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements.”

This policy replaces as of January 03, 2007, the existing BPA Manual Chapters 1110 and 1111 by combining them into one chapter and addressing limited personal use as a distinct subchapter for clarity.

This policy is supplemented by the Program Cyber Security Plan (PCSP) which is posted on the [Cyber Security site](#).

Questions regarding this policy should be sent to the [Cyber Security mailbox](#).

#### A. PURPOSE AND SCOPE

The purpose of this policy is to provide policy and procedures to federal and contractor employees and supervisors regarding the proper business-related use of BPA Information Technology (IT) Equipment. This policy provides notice to BPA federal and contractor employees and supervisors of the consequences for improper use of BPA IT Equipment. BPA IT Equipment represents a significant investment of BPA resources and its proper use is essential to the efficiency of the service that BPA provides.

This policy applies to all BPA federal and contractor employees. Contractor employee oversight or supervision is the responsibility of the contract company by which the contractor employee is employed. The conduct of the contractor employee in the performance of BPA business is subject to the contents of this Chapter and is managed through the contractual relationship between BPA and the contractor.

#### B. POLICY STATEMENT FOR BUSINESS-RELATED USE OF BPA IT EQUIPMENT

Except as provided by BPA Manual Chapter 1110A, BPA IT Equipment is to be used **only** by BPA federal and contractor employees who are Authorized System Users and **only** for BPA activities related to and consistent with the performance of BPA’s mission and in a manner approved by this policy and consistent with Cyber Security policy or by authorized BPA personnel to determine proper use when this policy does not speak to a particular issue. This policy is intended to apply whether the work of BPA federal and contractor employees is being done within the BPA work environment or working on BPA IT Equipment from a remote location.

#### C. RESPONSIBILITY FOR PROPER AND APPROPRIATE USE OF BPA IT EQUIPMENT

BPA federal and contractor employees are responsible for knowing and understanding current BPA policy regarding the use of BPA IT Equipment, including the limits to personal use established in Chapter 1110A, and conforming their use to such policy. BPA Supervisors are responsible for ensuring that BPA federal employees, under their supervision are current in their understanding of BPA policy regarding the use of BPA

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 10px 0 0 0;">Part: Information Management and Technology</p>	<p style="margin: 0;">Page 1110-6</p> <hr/> <p style="margin: 0;">Date 01/03/07</p>
--	---	---

IT Equipment, monitoring such use, and taking appropriate actions pursuant to BPA policy to correct improper use. Contracting Officers (COs)/Contracting Officer's Technical Representatives (COTRs) are responsible for ensuring that contractor employees through their contractor manager are current in their understanding of BPA policy regarding the use of BPA IT Equipment, monitoring such use, and taking appropriate actions to correct improper use.

**D. CONSEQUENCES OF IMPROPER USE OF BPA IT EQUIPMENT**

BPA federal and contractor employees having authorized access to BPA IT Equipment have an obligation to understand this policy and to limit their use to the activities it allows. BPA Supervisors and Contracting Officers (COs)/Contracting Officer's Technical Representatives (COTRs) have an obligation to understand this policy and monitor the activities of BPA federal and contractor employees, respectively, sufficiently to ensure that conduct is consistent with this policy. Failure of BPA federal and contractor employees or BPA Supervisors or the CO/COTR to satisfy their obligations may subject the employee to loss of authorized system use and/or in the case of BPA federal employees to possible disciplinary action. Contractor employees may be released in accordance with the contract terms. Improper use that is suspected of violating federal laws will be reported to the appropriate law enforcement agencies.

**E. POLICY REGARDING ALL BPA IT EQUIPMENT INVOLVING COMPUTERS**

The following guidelines are provided to BPA federal and contractor employees and BPA Supervisors as guidance for the proper use of BPA's IT Equipment. These guidelines do not constitute the totality of rules regarding proper use of BPA's IT Equipment involving computers. For circumstances not covered by these items, see BPA IT Equipment (BPAM 1110.3.B) and the [Cyber Security Office web site](#).

1. Only BPA provided and supported IT Equipment may be connected to BPA IT Equipment. This includes connections of desktop computer systems to BPA computer network and/or connections of any peripheral device to a desktop computer that is connected to the BPA computer network.
2. Only authorized BPA IT Support Staff is permitted to modify the configuration of settings for BPA IT Equipment, including computers. BPA federal and contractor employees may, however, change desktop presentation settings (e.g., wallpaper, screen resolution, speaker volume) as provided for by BPA-approved software. In addition, BPA federal and contractor employees may make modifications under the direction of the Help Desk when troubleshooting problems.
3. Only BPA Authorized Installers are permitted to install, modify, or move BPA IT Equipment. All other persons are not authorized to install, modify or move BPA IT Equipment. Unauthorized movement, modification or installation places the BPA IT Equipment being moved and the BPA computer network in jeopardy. In addition, the location of all BPA IT Equipment must be tracked under BPA's IT Equipment asset management program.
4. No software will be installed on BPA IT Equipment without proper authorization, which must include an approved Cyber Security review. This prohibition includes downloading executable files from the Internet, downloading software purchased by BPA federal and contractor employees for personal use, downloading freeware or shareware, downloading or receiving media for demonstration of Beta versions of software provided by outside vendors or provided by other BPA federal and contractor employees. A list of currently approved software is maintained by BPA's IT Program Management (NJM) organization.

**F. GUIDANCE SPECIFIC TO USE OF BPA'S E-MAIL SYSTEM**

Authorized system users are encouraged to communicate with others using BPA's e-mail whenever appropriate. However, its use is subject to the following guidelines which are provided to BPA federal and

	<h1>BPA MANUAL</h1> <h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p>Part: Information Management and Technology</p>	Page 1110-7
		Date 01/03/07

contractor employees and BPA Supervisors as guidance as to the proper use of BPA's e-mail system. These guidelines do not constitute the totality of rules regarding proper use of BPA's e-mail system. For circumstances not covered by these items, BPA federal and contractor employees and BPA Supervisors should consult the basic policy for use of BPA IT Equipment (BPAM 1110.3.B) and the [Cyber Security Office web site](#).

Cyber Security may disable an e-mail account that is in violation of BPA policy or that poses a threat to the BPA network. Cyber Security may be directed by the Supervisor to disable an e-mail account.

1. The BPA e-mail system and its contents, including attachments, are federal government property. As such, all messages sent with BPA's e-mail system, including those allowed by the Personal Use Allowance (BPAM Chapter 1110A), must be businesslike. Failure to use BPA's e-mail system in accordance with the above can put BPA and BPA federal and contractor employees at risk for legal liabilities, embarrassment, adverse business impacts, and other economic consequences. Upon request to Employee Relations, BPA Supervisors, have the right to review any e-mail messages, including attachments, put on the BPA e-mail system by BPA federal and contractor employees. Cyber Security and Cyber Security directed by law enforcement requests have the right to review any e-mail messages, including attachments, put on the BPA e-mail system by federal and contractor employees. BPA federal and contractor employees who have stored BPA e-mail on personally owned computing devices accept the obligation to make such e-mail available to Cyber Security.
2. BPA e-mail messages could become evidence in legal proceedings. If BPA federal and contractor employees' e-mail messages are requested under the Freedom of Information Act or litigation discovery process, BPA federal and contractor employees will be responsible for reviewing messages in their e-mail storage files and producing any responsive messages. If BPA federal and/or contractor employees store personal files not created for BPA work on BPA IT Equipment, then those files would be subject to disclosure.
3. BPA federal and contractor employees are responsible for the security of their individual BPA e-mail files and any e-mail messages they send using the BPA e-mail system. BPA federal and contractor employees should be aware that message recipients can forward the message to any number of individuals and messages may accidentally be delivered to the wrong recipient. In other words, when a BPA federal and/or contractor employee sends an e-mail message, the sending BPA federal and/or contractor employee has no control where the message may eventually go and who will read it. Care should be taken in both the preparation and sending of e-mail messages to minimize the risk that the messages will be received by unauthorized recipients. Messages sent using the BPA e-mail system and sent outside the BPA work environment will be identified as originating within BPA. Special care should be taken to ensure that such messages will only be received by intended recipients.
4. Because of the difficulty of ensuring complete security (see above), the BPA e-mail system should not be used to communicate sensitive unclassified information (SUI) without the proper safeguards authorized and provided by Cyber Security. When BPA e-mail is the only viable method of completing such communications, BPA federal and contractor employees should use extra care to ensure that the e-mail message is correctly addressed and that it will not be forwarded.
5. If the content of a BPA e-mail message possesses longer-term business value, BPA federal and contractor employees are encouraged to consider other methods of communicating the message, and if BPA e-mail is the appropriate method, to remove the e-mail message from the BPA e-mail system to a more permanent storage system. The minimum period of retention of BPA e-mail is thirty (30) days. All e-mail messages stored in the BPA e-mail system will be automatically purged (deleted) upon the

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 10px 0 0 0;">Part: Information Management and Technology</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Page 1110-8</td> </tr> <tr> <td style="padding: 5px;">Date 01/03/07</td> </tr> </table>	Page 1110-8	Date 01/03/07
Page 1110-8				
Date 01/03/07				

expiration of that minimum period or the period established by additional policy. Some e-mail messages may constitute Official Records. Specific guidance as to the retention of Office Records is provided in the [BPA Records Manual](#).

6. Only BPA's Standard e-mail services are authorized for installation and/or use on the BPA e-mail system. BPA federal and contractor employees are not authorized to install or access any other e-mail systems (e.g., accessing an e-mail service from the Internet or third-party provider). Use of any other e-mail system or services (e.g., an e-mail service from the Internet or a web-based e-mail system via BPA Internet services) is prohibited.
7. Auto-forwarding of e-mail from the BPA's e-mail system to any other e-mail system is prohibited. Auto-forwarding of a personal e-mail into the BPA e-mail system is also prohibited.
8. Only the BPA Security and Emergency Management Office, BPA Corporate Communications, and the Office of the Chief Information Security Officer (CISO) and such BPA employees and/or organizations designated by the BPA Administrator are permitted to use the BPA e-mail system to broadcast messages. Otherwise, BPA federal and contractor employees are not permitted to use the group addressing capability of the BPA e-mail system to broadcast e-mail messages.
9. Using the BPA e-mail system for fund-raising activities other than by authorized BPA employees is prohibited.
10. Sending any passwords in an e-mail or as an attachment using the BPA e-mail system is prohibited unless the e-mail is encrypted with authorized BPA encryption software. Use of encryption must be approved by Cyber Security.
11. Sending Privacy Act of Personally Identifiable Information (PII) in an e-mail or as an attachment using the BPA e-mail system is prohibited unless the e-mail is encrypted with authorized BPA encryption software. Use of encryption must be approved by Cyber Security.
12. The BPA e-mail system may not be used for any illegal activity as defined by state or federal law, regardless of whether or not the state law applies to BPA. State laws shall include all the states in which BPA operates in which BPA is subject to by contract.
13. The BPA e-mail system may not be used to distribute chain e-mails (i.e., electronic chain letters).

#### **G. GUIDANCE SPECIFIC TO USE OF BPA'S INTRA/INTERNET EQUIPMENT**

The following items are provided to BPA federal and contractor employees and BPA Supervisors as guidance to the proper use of BPA's Internet Equipment. This list of guidance items does not constitute the totality of rules regarding proper use of BPA's Internet Equipment. For circumstances not covered by these items, BPA federal and contractor employees and BPA Supervisors should consult the basic policy for use of BPA IT Equipment (BPAM 1110.3.B) and consult with their supervisors and Cyber Security.

1. Because of the continuous and dynamic risk inherent in the necessary connection between BPA Intra- and Internet and the Internet as a whole, BPA is continuously assessing, altering, adjusting and revising its policies and technologies to ensure the security of BPA's Intra- and Internet connections. Cyber Security continuously monitors Internet access and may block access to any Internet site it determines may create an unacceptable risk to BPA.
2. Upon the Supervisor's (federal employees) or the CO/COTR's (contractor employee) or law enforcement's request or as result of an intrusion detection alert or monitoring alert, Cyber Security may at its discretion review an individual's Internet usage.

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 0;">Part: Information Management and Technology</p>	<p style="margin: 0;">Page 1110-9</p> <hr/> <p style="margin: 0;">Date 01/03/07</p>
--	--	---

3. Internet posting of BPA business or security-related information, which includes BPA e-mail addresses, sensitive information or PII, for access either internally or externally is prohibited without authorization. This prohibition applies to static postings and to interactive postings, such as “blog” or “chat room” sites.
4. Because of the mechanics of some kinds of Internet searches, BPA federal and contractor employees who encounter data during authorized, business-related Internet searches that is reasonably likely to violate federal law and/or BPA policy regarding proper use of BPA IT Equipment, should report the occurrence to their BPA Supervisors and/or to the BPA Cyber Security organization and follow instructions from those authorities for preventing recurrence. If BPA federal and contractor employees are notified either electronically or otherwise that their search activities have encountered such data, they should immediately cease and desist from such search and, if necessary, consult with Cyber Security as to how their authorized search activity may be conducted without causing such encounters.
5. BPA federal and contractor employees’ personal (non-business-related) use of BPA Internet Equipment should strictly adhere to the limits set forth in BPAM Chapter 1110A.
6. The following use of BPA’s Internet connection is strictly prohibited and such use may result in disciplinary action: (1) accessing and/or downloading any form of pornography or sexually explicit, or offensive material; (2) accessing on-line gambling or gaming web sites and/or engaging in any on-line gambling or gaming.
7. The following use of BPA’s Internet connection is strictly prohibited unless previously approved and supported by Cyber Security policy: accessing and conducting financial transactions in any form.

**H. GUIDANCE SPECIFIC TO USE OF BPA’S REMOTE ACCESS EQUIPMENT**

The following items are provided to BPA federal and contractor employees and BPA Supervisors as guidance on to the proper use of BPA’s Remote Access Equipment. This guidance does not constitute the totality of rules regarding proper use of BPA’s Remote Access Equipment. For circumstances not covered by this guidance, BPA federal and contractor employees should consult the basic policy for use of BPA IT Equipment (BPAM 1110.3.B) and consult with their supervisors.

1. The office of the Chief Information Security Officer (CISO) manages the approval of Remote Access Service. Verification, provided by BPA Supervisors, of the business need for Remote Access Services will be required prior to granting authorization.
2. Using BPA IT Equipment via Remote Access Services for personal (non-business-related) use shall strictly adhere to the limits set forth in Chapter 1110A.
3. Authorized connections to BPA IT Equipment using Remote Access Services must be terminated as soon as the need for the use has ceased. Remaining connected to BPA IT Equipment using Remote Access Services for extended periods when there is no need for the connection ties up limited resources. Such connections, when detected will be terminated unless specifically authorized through Cyber Security.
4. Use of non-BPA IT Equipment for remote access is strictly prohibited.

**Chapter 1110A: Allowance for Limited Personal Use of BPA Information Technology (IT) Equipment**

**A. PURPOSE**

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 10px 0 0 0;">Part: Information Management and Technology</p>	<p style="margin: 0;">Page 1110-10</p> <hr/> <p style="margin: 0;">Date 01/03/07</p>
--	---	--

The purpose of this allowance and exception from BPA's otherwise business-only policy with regards to the use of BPA IT Equipment is to provide guidance to BPA federal and contractor employees and BPA Supervisors regarding the proper personal use of BPA IT Equipment. BPA IT Equipment represents a significant investment of resources by BPA and proper use is essential to the efficiency of the service which BPA was created to provide. BPA federal and contractor employees having access to BPA IT Equipment have an obligation to understand this policy and to limit their use to the activities it allows. BPA Supervisors have an obligation to understand this policy and monitor the activities of their employees sufficiently to ensure that policy limits are adhered to. Failure of BPA federal and contractor employees or BPA Supervisors to satisfy their obligations may subject them to loss of system access, disciplinary actions, and/or immediate contract termination.

This allowance does not modify the requirements of the Standards of Ethical Conduct for employees of the Executive Branch [Title 5 Code of Federal Regulations (CFR), 2635], including the employee's responsibility to protect and conserve Government property, to use it for authorized purposes only, and to use official time in an honest effort to perform official duties [5 CFR 2635.704(a) and (b)]. Nothing in BPAM Chapter 1110A pertains to or restricts use of Government property by an employee to carry out his or her official duties and responsibilities in furtherance of the mission of BPA.

**B. POLICY STATEMENT RELATED TO PERSONAL USE OF BPA IT EQUIPMENT**

BPA IT Equipment is to be used only for supervisor-authorized activities related to and consistent with the performance of BPA's mission, subject to the limited personal use allowance provided below.

**C. LIMITED PERSONAL USE ALLOWANCE**

Personal use of designated BPA IT Equipment is allowed within the limits and prohibitions specified in this policy. This allowance does not grant or create an inherent right to use Government resources, and one should not be inferred.

Any personal use, even if ostensibly allowed by this policy, may be further limited or revoked at any time by BPA Supervisors or Cyber Security when circumstances warrant such action.

**D. RESPONSIBILITY FOR PROPER AND APPROPRIATE PERSONAL USE OF BPA IT EQUIPMENT**

BPA federal and contractor employees are responsible for knowing and understanding current BPA policy regarding the use of BPA IT Equipment, including the limits to the allowance for limited personal use established by BPAM Chapter 1110A, and conforming their use to such policy. BPA Supervisors are responsible for

1. ensuring that BPA federal and contractor employees under their supervision and/or direction remain continuously current in their understanding of BPA policy regarding the use of BPA IT Equipment;
2. monitoring potential misuse as appropriate in conjunction with Cyber Security and Employee Relations; and
3. taking appropriate actions pursuant to BPA policy to correct inappropriate use when inappropriate use is observed or reported.

**E. CONSEQUENCES OF IMPROPER PERSONAL USE OF BPA IT EQUIPMENT**

Failure of BPA federal and contractor employees or BPA Supervisors to satisfy their responsibility for proper and appropriate personal use of BPA IT Equipment may subject them to loss of system access and/or possible disciplinary actions or immediate contract termination.

	<h1>BPA MANUAL</h1>	Page 1110-11
	<h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p>Part: Information Management and Technology</p>	Date 01/03/07

### F. APPLICATION OF NATIONAL SECURITY LEVELS TO LIMITED PERSONAL USE ALLOWANCE

The limited personal use allowance stated in BPAM Chapter 1110A.C applies to all BPA IT Equipment only when the national security level has been designated as Green. The allowance is further limited when the national security levels are other than Green as follows:

1. When the national security level has been designated as Orange or Red, there shall be no personal use of BPA IT Equipment unless otherwise authorized by Cyber Security.
2. When the national security level has been designated as Yellow, personal use allowance shall be permitted on BPA IT Equipment. However, web site and e-mail blocking may increase as the result of DOE, Homeland Security and other official advisories. Should increased web site and e-mail blocking become necessary, Cyber Security shall use official communication channels to notify the workforce in general provided such advisories are not sensitive or classified.
3. When the national security level has been designated as Green or Blue, the personal use policy shall be permitted on BPA IT Equipment. However, web site and e-mail blocking may increase as the result of DOE, Homeland Security and other official advisories. Should increased web site and e-mail blocking become necessary, Cyber Security shall use official communication channels to notify the workforce in general provided such advisories are not sensitive or classified..
4. In situations, where National Security Levels are not modified but there is a credible threat reported by law enforcement, Homeland Security, or the DOE Inspector General or DOE incident response (CIAC) or other official sources, Cyber Security may revoke limited personal use authorization throughout BPA until the threat has been cleared. Prior and subsequent to revocation or the threat being cleared, Cyber Security shall notify the workforce through official BPA channels.

### G. SPECIFIC PROHIBITIONS

In all cases, personal use of BPA IT Equipment on duty time is prohibited. That is, personal use of BPA IT Equipment is only permitted before the workday begins, after the workday ends or during lunch time. The following specific restrictions apply to BPA federal and contractor employees' personal use of BPA IT Equipment:

1. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment for any personal use that interferes with employees' official duties or reflects badly on the conduct of the federal service (this prohibition includes the use of language that would reflect badly on the federal service in otherwise allowed personal use instances). The prohibition especially prohibits gambling and the viewing or correspondence about and/or trading or procurement of weapons of any kind.
2. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment for any personal use that has been made unlawful by federal, state or local law (whether or not such state or local law governs the conduct of BPA as a federal agency).
3. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment to maintain or support a personal private business or to assist family, friends or other persons in such activities.
4. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that violates the Standards of Ethical Conduct for Government employees.



# BPA MANUAL

## Chapter 1110: Business Use of BPA Information Technology Services Policy

Part: Information Management and Technology

Page  
1110-12

Date  
01/03/07

5. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment in a way that expressly or impliedly represents that BPA or the federal government has sanctioned or endorsed the specific purpose of the personal use.
6. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that communicates an express or implied threat or violates BPA's Harassment-Free Workplace Policy.
7. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that includes communication of material (language and/or pictures) that a reasonable person would find offensive (e.g., hate speech, material that ridicules others on the basis of race, gender, color, religion, disability, national origin, sexual orientation, educational and/or economic level).
8. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that creates a risk to BPA IT Equipment systems (e.g., when such use creates or increases the possibility of threats to BPA IT Equipment by malicious software [Malware]).
9. BPA federal and contractor employees are specifically prohibited from personal use of Operational and Control IT Equipment such as Instrument Controllers (ICs) under any circumstances.
10. While offsite, BPA federal and contractor employees are not permitted to use BPA IT Equipment to connect "directly" to the Internet using a modem (dial up), wireless or wired connection. All connections must be made to the BPA administrative network using VPN software or authorized software. A violation may result in the revocation of remote access privileges.
11. BPA federal and contractor employees are specifically prohibited from removing BPA IT Equipment from the BPA work environment in order to use such equipment for personal use. However, when there is a BPA business requirement to relocate BPA IT Equipment, such relocation may be done through the BPA established processes.
12. BPA federal and contractor employees are specifically prohibited from making purchases of any product for personal use using BPA IT Internet Equipment.
13. BPA federal and contractor employees are specifically prohibited from personal use of any BPA IT Equipment that is designated for classified use under the National Security Act.
14. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment that imposes more than minimal additional expense to BPA unless authorized by BPA.
15. BPA federal and contractor employees are specifically prohibited from any personal use of BPA IT Equipment that gives the impression that the user is acting in an official capacity.
16. BPA federal and contractor employees are specifically prohibited from any personal use that requires the downloading (i.e., copying) from any non-BPA IT or BPA IT Equipment of large files (greater than five megabytes) such as documents, attachments, motion or still images, digital audio files, and data into BPA IT Equipment.
17. BPA federal and contractor employees are specifically prohibited from any personal use of a program or Internet site that provides continuous data streams to BPA IT Equipment, even if such streams are not stored as files within BPA IT Equipment (e.g., continuous stock quotes, radio broadcasts, news headlines, weather, etc.).
18. BPA federal and contractor employees are specifically prohibited from creating, downloading, viewing, storing, copying or transmitting sexually explicit or sexually oriented materials using BPA IT Equipment.



# BPA MANUAL

## Chapter 1110: Business Use of BPA Information Technology Services Policy

Part: Information Management and Technology

Page  
1110-13

Date  
01/03/07

19. BPA federal and contractor employees are specifically prohibited from participation in fundraising for any entity or activity other than authorized activity related to the Combined federal Campaign or Associates Functions using BPA IT Equipment.
20. BPA federal and contractor employees are specifically prohibited from participation in any political activity using BPA IT Equipment.
21. BPA federal and contractor employees are specifically prohibited from modification of BPA IT Equipment in any way to facilitate personal or BPA official business use.
22. BPA federal and contractor employees are specifically prohibited from installation of any non-BPA owned software or hardware devices on BPA IT Equipment to facilitate personal use.
23. BPA federal and contractor employees are specifically prohibited from any frequent personal use that may cause congestion, delay, or disruption of service to any BPA IT Equipment, including greeting cards, audio, and streaming video and audio, etc., unless authorized by Cyber Security.
24. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment that involves unauthorized acquisition, use, reproduction, transmission, or distribution of controlled information (e.g., computer software and data; classified, business sensitive, or other nonpublic data; proprietary data; export controlled software or data; or any information in violation of the Privacy Act, copyright, trademark, or other intellectual property rights beyond fair use).
25. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment that involves gaining authorized access to internal or external systems or networks.

### H. NO PRIVACY EXPECTATION FOR PERSONAL USE

BPA federal and contractor employees should understand that there is no right and should be no expectation of privacy. BPA federal and contractor employees' use of BPA IT Equipment is always subject to supervision and such supervision may include supervisory review, including active monitoring through the use of monitoring tools, of BPA federal and contractor employees' use of BPA IT Equipment and the content of materials stored within BPA IT Equipment. Personal use of BPA IT Equipment by BPA federal and contractor employees implies consent by such employees to such review. BPA federal and contractor employees who wish their personal use activities to be private should not use BPA IT Equipment for personal use.

BPA federal and contractor employees should further understand that the content, whether personal or work related, stored within BPA IT Equipment is the property of BPA and may be disclosed in response to a valid subpoena, warrant, court order (including litigation discovery request), Freedom of Information Act (5 USC 552) request, or other authorized direction (e.g., BPA federal and contractor employees' supervisor, Cyber Security, Inspector General, etc.).

### I. GUIDANCE FOR ALLOWED PERSONAL USE

The following examples are provided solely for the purpose of guidance for BPA federal and contractor employees and BPA Supervisors to understand what may be allowed as personal use of BPA IT Equipment. BPA federal and contractor employees and BPA Supervisors should not rely on these examples as specific grants of authority for the uses described. If BPA federal and contractor employees or BPA Supervisors are in doubt about whether a specific personal use is or is not allowed by this policy, they should always seek specific authority from their supervisors and/or Cyber Security.

#### Examples:



# BPA MANUAL

Page  
1110-14

## Chapter 1110: Business Use of BPA Information Technology Services Policy

Date  
01/03/07

Part: Information Management and Technology

1. Occasionally during work and non-work hours using e-mail or telephone, including voice mail, to keep in touch with family members/or significant others regarding work and/or school schedules (e.g., BPA federal and contractor employees calls or e-mails spouse to inform spouse she will be required to work overtime; BPA federal and contractor employee calls or e-mails dependant's school to confirm time of parent-teacher meeting, etc.). Occasional use is less than ten minutes during duty time unless otherwise authorized by a supervisor. Occasional use in this context are times outside of the non-work time definition.
2. Using e-mail or telephone to check on status of bank, credit union or TSP accounts under the non-work time definition not to exceed two (2) continuous hours in any non-work period.
3. Preparing and storing current resume and related materials on the local hard drive only under the non-work time definition with no time limit.
4. Accessing public library, newspaper and similar publicly available data that does not include downloading (copying) significant amounts of data or printing numerous or large documents on BPA printers under the non-work time definition not to exceed two (2) continuous hours in any non-work period. Any downloading of data must be to the local hard drive and must not occupy more than fifteen (15) percent of the available hard drive storage space.
5. Conducting research regarding personal travel arrangements or consumer matters (e.g., Kelly Blue Book information) on web sites under the non-work time definition not to exceed two (2) continuous hours in any non-work period.
6. Checking current or predicted weather on web sites under the non-work time definition not to exceed two (2) continuous hours in any non-work period.
7. Personal electronic images may be stored on the local hard drive but not on the H: drive or any other network drive, provided such photographs do not occupy more than fifteen (15) percent of the total data storage on the local hard drive, have been scanned for malicious software and are not in violation of any federal or state laws, regulations, policies or DOE Orders.
8. All BPA federal and contractor employees are permitted to use BPA IT Equipment for reasonable personal use via Remote Access Services (Dial-up, Internet, Wireless) on official travel status and in conjunction with a valid telecommuting agreement. The user must access the Internet through an authorized BPA access point using either the VPN software for wired and wireless connections or the authorized software for dial-up. Failure to follow this process may result in the revocation of remote access privileges.

### 1110.4 RESPONSIBILITIES

- A. Federal and contractor Employees** are responsible for the knowledge and the understanding of current BPA policy regarding the use of BPA IT equipment, including the limits of personal use, established in Cyber Security Chapter 1110.A, and are to conform to the use of such policy. BPA federal and contractor employees, who have authorized access to BPA IT equipment, have an obligation to understand this policy and to limit their use to the activities as allowed. Failure of BPA **federal and contractor employees** or BPA supervisors or CO/COTRs to satisfy their obligations, may subject the employee to loss of authorized system use and/or in the case of BPA federal employees to possible disciplinary action.

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 10px 0 0 0;">Part: Information Management and Technology</p>	Page 1110-15
		Date 01/03/07

- B. Supervisors** are responsible for ensuring that BPA ***federal employees***, under their supervision are current in their understanding of BPA policy regarding the use of BPA IT equipment, monitoring such use, and taking appropriate actions pursuant to BPA policy to correct improper use. BPA supervisors have an obligation to understand this policy and monitor the activities of BPA federal employees sufficiently to ensure that their conduct is consistent with this policy.
- C. Contracting Officers (CO) and Contracting Officer Technical Representatives (COTRs)** are responsible for ensuring that ***contractor employees*** working through their contractor manager, are kept current in their understanding of BPA policy regarding the use of BPA IT equipment, monitoring such use, and taking appropriate actions to correct improper (inappropriate) use. BPA Contracting Officers (COs)/Contracting Officer Technical Representatives (COTRs) have an obligation to understand this policy and monitor the activities of ***contractor employees*** sufficiently to ensure that their conduct is consistent with this policy. ***Contractor employees*** who do not comply with the policy may be released in accordance with the contract terms.
- D. Contractors** are responsible for oversight or supervision of the ***contractor employees*** and ensuring adherence to these policies.

### 1110.5 PROCEDURES

No information in this section.

### 1110.6 REFERENCES

- A. Pub. L. No. 93-579, Title 5 U.S.C. § 552a, Privacy Act of 1974 (2000)**
- B. Pub. L. No. 107-347, Title III, 44 U.S.C. § 3544 (a)(3)(C), Information Security, Federal Information Security Management Act of 2002**
- C. 5 CFR § 2635, Standards of Ethical Conduct for Employees of the Executive Branch**
- D. 5 CFR § 2635.704(a) and (b), Standards of Ethical Conduct for Employees of the Executive Branch**
- E. US-DOE: Protection of Sensitive Unclassified Information, Including Personally Identifiable Information, September 6, 2006**
- F. BPA Manual Chapter 400/700A, Appendix A, BPA's Harassment-Free Workplace Policy**
- G. BPA Program Cyber Security Plan (PCSP)**
- H. Cyber Security Policy BPA-20060809-001, Personally Identifiable Information (PII)**

	<h1>BPA MANUAL</h1>	<b>Page:</b> 1140-1
	<h2>Chapter 1140: Use of Social Media / Web 2.0 tools</h2>	<b>Date:</b> 01/19/10
Part: Information Management and Technology		

### 1140.0 PURPOSE:

This chapter authorizes Bonneville Power Administration's (BPA) Chief Public Affairs Officer (CPAO) to issue policies on the use of Social Media and Web 2.0 Technologies that apply throughout BPA. This chapter addresses the appropriate use of Social Media/Web 2.0 tools to deliver information and to engage our customers and the general public in active, two-way discussions of issues important to BPA and its stakeholders.

### 1140.1 DEFINITIONS

**A. Authorized Use:** Use of Social Media / Web 2.0 technologies by a person or persons approved by the CPAO (or delegate) to provide information and engage the public on behalf of BPA.

**B. Social Media (SM):** Social Media is an umbrella term that defines the various Internet platforms that integrate technology, social interaction, and content creation. Social Media use the "wisdom of crowds" to connect information in a collaborative manner online. Through Social Media, individuals or collaborations of individuals create Web content, organize content, edit or comment on content, combine content, and share content. Examples include blogs, Facebook and MySpace pages, and YouTube accounts.

**C. W2.0 Technologies:** Technologies enabling Social Media, including [RSS](#) (Really Simple Syndication) and other syndicated Web feeds, [blogs](#), wikis, photo-sharing, video-sharing, [podcasts](#), mashups, widgets, virtual worlds, micro-blogs, and other methods of digital interaction with the public.

**D. Unauthorized Use:** Use of Social Media / Web 2.0 technologies by a person or persons not approved by the CPAO to provide information and engage the public on behalf of BPA. Unauthorized use includes on or off-duty use by a non-approved person to speak on behalf of BPA. Unauthorized use could result in discipline up to and including removal from federal service.

**E. Inappropriate Use:** Use of Social Media / Web 2.0 technologies by any employee or contractor in violation of BPA policies, including Information Technology Policies, Policy for Business Use of BPA Information Technology, and BPA's Harassment Free Workplace Policy. Inappropriate use could result in discipline up to and including removal from federal service.

**F. CPAO or other other organizational heads:** For purposes of this policy, the responsibilities for authorizing, approving or reviewing could be delegated one level from the authorizing position.

	<h1>BPA MANUAL</h1>	<b>Page:</b> 1140-2
	<h2>Chapter 1140: Use of Social Media / Web 2.0 tools</h2>	<b>Date:</b> 01/19/10
Part: Information Management and Technology		

### 1140.2 POLICY

BPA Public Affairs will create and maintain Social Media sites for authorized use. Any organization within BPA wishing to use Social Media for official purposes must receive initial approval by the CPAO. Continuing review and approval of specific uses will be the responsibility of the requesting organizational head, with periodic review by the CPAO. For example, after initial approval for use in recruitment, the Chief Human Capital Officer will have responsibility for continuing review and approval of recruitment-related uses.

Authorized BPA Social Media sites, communication, and content must clearly identify ownership or sponsorship through the use of BPA branding. The planned BPA branding strategy must be included in initial requests for CPAO approval.

All existing BPA policies, such as the Harassment-Free Workplace Policy, apply to use of SM/W2.0 technologies.

### 1140.3 RESPONSIBILITIES

**A. CPAO:** BPA's CPAO must review and approve all initial requests for authorized use of SM/W2.0 technologies, including but not limited to blogs, Twitter, YouTube, Facebook and MySpace. In addition, BPA's CPAO is responsible for BPA's coordinated and integrated corporate branding.

**B. Information Technology (IT):** IT and Cyber Security will assist, when appropriate, to make these technologies available on the the external BPA Web site and accessible on BPA equipment for those with "official and authorized" communication responsibilities.

**C. BPA Business Units and Organizations:** All organizations must seek approval from the CPAO for authorized use of SW/W2.0 technologies. The planned BPA branding strategy must be included in initial requests for use of the SM/W2.0 technologies.

Continued review and approval for specific uses will be the responsibility of the requesting organizational head, with periodic review by the CPAO.

**D. Employess and contractors:** Employees and contractors must obtain approval from their direct management before seeking approval from the CPAO for authorized use of SW/W2.0 technologies. This includes approval to incorporate BPA identifiers in their profile or user name (i.e., William@bpa). Employees and contractors must adhere to all BPA policies.

	<h1>BPA MANUAL</h1>	<b>Page:</b> 1140-3
	<h2>Chapter 1140: Use of Social Media / Web 2.0 tools</h2>	<b>Date:</b> 01/19/10
Part: Information Management and Technology		

### 1140.4 PROCEDURES

**A.** BPA uses Social Media/Web 2.0 (SM/W2.0) technologies to enhance public communications and information exchange in support of BPA’s mission. These tools are evolving rapidly and are shaping how we work with our customers, business partners, other government agencies, and the public.

**B.** Authorized BPA use of a particular SM/W2.0 technology requires approval by the CPAO. Requesting organizations must submit a strategic communications plan and commit the resources necessary to manage and maintain the Social Media engagement.

**C.** The guidelines established in this document are designed to ensure that authorized BPA Social Media accounts present accurate, credible information and that personal opinions are not allowed to be portrayed as official BPA positions. Due to the nature of Social Media tools and the free exchange of information and ideas, BPA will indicate in all SM/W2.0 accounts possible that “For official BPA information go to [www.bpa.gov](http://www.bpa.gov).”

**D.** Several SM/W2.0 technologies allow or encourage the submission of written comments. BPA encourages this public interaction / engagement.

1. A manager requesting CPAO approval for Social Media use must specify whether interaction / engagement with the public is desired.
2. For Social Media sites allowing public interaction, BPA will post a notice encouraging users to stay focused, be respectful, and avoid offensive posts. BPA will be bound by the terms of service for the particular Social Media provider and will notify the provider of inappropriate posts . BPA will not put in place additional content restrictions.
3. Individuals commenting in their authorized capacity on any Social Media platform must identify their relationship to BPA.
4. Employees and contractors engaged in their authorized use should follow the same rules of behavior they would when participating in a public meeting or serving as an official BPA spokesperson.

**E.** BPA employees and contractors engaged in authorized use are expected to fact check communications and, whenever feasible, to correct inaccurate information about BPA.

**F.** Authorized use of SM/W2.0 technologies must adhere to all applicable statutes, regulations, and directives governing official government use of information and information technology. These statutes and regulations include, but are not limited to, the Federal Records Act, the Freedom of Information Act, the Privacy Act, the Federal Advisory Committee Act (FACA), the Paperwork Reduction Act (PRA), and the

	<h1>BPA MANUAL</h1> <h2>Chapter 1140: Use of Social Media / Web 2.0 tools</h2> <p>Part: Information Management and Technology</p>	<b>Page:</b> 1140-4
		<b>Date:</b> 01/19/10

Americans with Disabilities Act. BPA federal and contract employees may not use or post materials protected under intellectual property laws (copyright, patents, etc.) without written permission from the intellectual property owner.

**G.** All SM/W2.0 postings seeking public interaction require posting of the the following Comment Policy Statement where possible.

### Comment Policy:

BPA welcomes you to share your comments, ideas and concerns. However, please respect other readers and contributors by following these general rules of civil discourse.

- **Stay focused.** All viewpoints are welcome, but comments should remain relevant to the Bonneville Power Administration or BPA-related topics. Please keep your comments on topic.
- **Be respectful.** Personal attacks, profanity, aggressive behavior or unsupported accusations are not only harmful to the conversations, they may be in violation of the rules of this forum.
- **Add value.** Comments should be relevant. The best way to be interesting and garner attention is to write about what you know. If you have a deep understanding of something, talk about the benefits, challenges and issues around it. Try not to rant about things you don't understand, as you're more likely to get embarrassed by a real expert.
- **No spam.** Repeated posting of identical or very similar content or promoting products or services is counterproductive and may be in violation of the rules of this forum.

Users are responsible for any and all comments that they submit. All posted comments are in the public domain.

BPA does not guarantee or warrant that any information posted by individuals on this Web site is correct and disclaims any liability for any loss or damage resulting from reliance on any such information. BPA assumes no liability for anything posted on this Web site. **For official BPA information visit [www.bpa.gov](http://www.bpa.gov) .**

Reporters are asked to send questions to the BPA media office through their normal channels and refrain from submitting questions in this forum.

BPA reserves the right to modify this policy at any time.

### 1140.5 REFERENCES:

**A. BPAM Chapter 1101** Information Technologies Policies

	<h1>BPA MANUAL</h1> <h2>Chapter 1140: Use of Social Media / Web 2.0 tools</h2>	<b>Page:</b> 1140-5
	<p>Part: Information Management and Technology</p>	<b>Date:</b> 01/19/10

**B. BPAM Chapter 1110** Policy for Business Use of BPA Information Technology Services

**C. BPA's Harassment Free Workplace Policy**

PLEASE hover over Row 2 title names, a comment box will appear with an explanation of the associated column. Missing data in an occupied row means it was not available. However, the data is included under the assumption that the actions were implemented during the requested time frame.

Rule Name	Source - Block IPs & Networks	Destination - for all listed Source IPs	Details	Requestor	Date	CRM/CMS	Tech	ACTION
Cyber Security Blocked Networks created 04/08/08 Ex 6	114.249.17.85	ANY	capestonecounty		10/17/2011	CMS 97284		DROP
	123.117.21.38		flewlyinghome		10/17/2011	CMS 97284		DROP
	206.183.111.97		Duqu backchannel IP		10/20/2011	CMS 97284		DROP
	209.85.51.152		Blocked per Cyber request	Ex 6	9/15/2011		Ex 6	DROP
	217.218.67.227		Added per	Ex 6	10/9/2012		Ex 6	DROP
	61.218.36.21		Added per		2/13/2012			DROP
	64.202.189.170		happybehere		10/17/2011	CMS 97284		DROP
	71.9.27.11				1/5/2012			DROP
	74.117.180.216		Blocked per Cyber request		9/15/2011			DROP
	74.91.218.117		Blocked per Cyber request		9/15/2011			DROP
87.106.193.21		Blocked per Cyber request		9/15/2011			DROP	
Cyber Blocked Servers created 01/19/10 Ex 6	12.163.32.15	ANY	ie.aq1.co.uk:80	Ex 6	9/18/2012		Ex 6	DROP
	62.152.104.149		hxxp://62.152.104.149/public/help/exploit.html		9/18/2012			DROP
Cyber Blocked Networks 2 created 7/7/?? per Cyber DOE request	119.177.69.124	ANY			9/9/2011			DROP
	119.255.28.229				9/9/2011			DROP
	125.71.200.13				9/9/2011			DROP
	202.194.15.141			Ex 6	9/9/2011		Ex 6	DROP
	218.59.217.165				9/9/2011			DROP
	220.181.94.222				9/9/2011			DROP
	221.3.109.230				9/9/2011			DROP
	222.35.143.118				9/9/2011			DROP
	222.66.175.251				9/9/2011			DROP
	61.160.201.26				9/9/2011			DROP
	72.167.0.128				4/11/2012	CMS 103995		DROP
209.59.175.67		regwork.exe		4/11/2012			DROP	
Cyber Blocked Networks 3 created 12/2/11 per cyber DOE request	168.144.38.132	ANY			12/2/2011			DROP
	184.22.45.17				12/2/2011			DROP
	209.236.123.83				12/2/2011			DROP
	64.34.23.82				12/2/2011			DROP
Cyber Blocked Networks 4 created 2/1/2013 Blocked per Cyber Ex 6	174.59.172.19	ANY	Blocked per Cyber		2/1/2013			DROP
	189.44.195.27		Blocked per Cyber		2/1/2013			DROP
	190.242.109.195		Blocked per Cyber		2/1/2013			DROP
	200.195.135.14		Blocked per Cyber		2/1/2013			DROP
	211.106.171.83		Blocked per Cyber		2/1/2013			DROP
	211.174.163.103		Blocked per Cyber		2/1/2013		Ex 6	DROP
	216.183.175.3		Blocked per Cyber		2/1/2013			DROP
	46.22.130.121		Blocked per Cyber		2/1/2013			DROP
	59.18.102.227		Blocked per Cyber		2/1/2013			DROP
	66.209.50.141		Blocked per Cyber		2/1/2013			DROP
	77.109.1.20		Blocked per Cyber		2/1/2013			DROP
89.189.38.140		Blocked per Cyber		2/1/2013			DROP	

1	<a href="http://www.google.com/earth/explora/products/plugin.html">http://www.google.com/earth/explora/products/plugin.html</a> <a href="http://www.google.com/earth/plugin/error.html">http://www.google.com/earth/plugin/error.html</a> ^.*earth/plugin/GoogleEarthPluginSetup.exe (RegEx)	CRM 1713280; Ex 6 (BPA) - NJST-TPP-1	Added on 07/05/12
2	http://217<dot>218<dot>67<dot>227 https://217<dot>218<dot>67<dot>227 http://english<dot>khamenei<dot>ir https://english<dot>khamenei<dot>ir	This was requested by Ex 6	Added on 10/09/12
3	http://www.gnnet[.]co[.]kr http://server[.]birdfollow[.]com http://mp3[.]nilukco[.]com http://service[.]birdfollow[.]com  https://www.gnnet[.]co[.]kr https://server[.]birdfollow[.]com  https://mp3[.]nilukco[.]com https://service[.]birdfollow[.]com	This was requested by Ex 6	Added on 02/01/13
4	http://downloadsrv[.]servftp[.]com https://downloadsrv[.]servftp[.]com	This was requested by Ex 6	Added on 02/05/13

<b>Category Name</b>	<b>Default Action</b>
Abortion	Quota
Abortion > Pro-Choice	Quota
Abortion > Pro-Life	Quota
Advocacy Groups	Quota
Miscellaneous > Dynamic Content	Permit
Miscellaneous > Images (Media)	Permit
Miscellaneous > Network Errors	Permit
Miscellaneous > Private IP Addresses	Permit
Security > Bot Networks	Block
Security > Malicious Websites	Block
Security > Keyloggers	Block
Security > Potentially Unwanted Software	Block
Society & Lifestyles > Social Networking & Personal Sites	Block
Special Events	Quota

<b>SurfControl Category</b>	<b>BPA Rule</b>
Adult/Sexually Explicit	Disallow
Advertisements & Popups	Disallow
Alcohol & Tobacco	Disallow
Chat	Disallow
Criminal Activity	Disallow
Downloads	Disallow
Gambling	Disallow
Games	Disallow
Hacking, Spyware	Disallow
Illegal Drugs	Disallow
Intimate Apparel & Swimwear	Disallow
Intolerance & Hate	Disallow
Peer-to-Peer	Disallow
Personals & Dating	Disallow
Phishing & Fraud	Disallow
Proxies & Translators	Disallow
Ringtones/Mobile Phone Downloads	Disallow
Sex Education	Disallow
Spam URLs	Disallow
Spyware	Disallow*
Tasteless & Offensive	Disallow
Violence	Disallow
Weapons	Disallow
Web-based E-mail	Disallow

<b>Corresponding Websense Category (or categories)</b>	<b>Default Action</b>
Adult Material > Adult Content	Block
Adult Material > Nudity	Block
Adult Material > Sex (1)	Block
Productivity > Advertisements	Block
Society & Lifestyles > Alcohol & Tobacco	Quota
Internet Communication > Web Chat	Block
Productivity > Instant Messaging	Block
Illegal or Questionable	Block
Entertainment > MP3 & Audio Download Services	Block
Miscellaneous > File Download Servers	Permit
Productivity > Freeware & Software Download	Block
Gambling	Block
Games	Block
Information Technology > Hacking	Block
Drugs	Block
Drugs > Abused Drugs	Block
Drugs > Marijuana	Permit
Adult Material > Lingere & Swimsuit	Confirm
Raciam & Hate	Block
Militancy & Extremist	Block
Bandwidth > Peer-to-Peer Filesharing	Block
Society & Lifestyles > Personals & Dating	Quota
Security > Phishing & Other Frauds	Block
Information Technology > Proxy Avoidance	Block
Information Technology > URL Translation Sites	Block
Productvity > Freeware & Software Download	Block
Adult Material > Sex Education	Permit
Security > Phishing & Other Frauds	Block
Security > Spyware	Block
Tasteless	Block
Violence	Block
Weapons	Block
Internet Communication > General Email	Confirm
Internet Communication > Organizational Email	Permit
Internet Communication > Text & Media Messaging	Permit

<b>SurfControl Category</b>	<b>BPA Rule</b>
Arts	Allow
Blogs & Forums	Allow
Business	Allow
Company & Internet	Allow
Computing & Internet	Allow
Custom Categorization	Allow
Education	Allow
Entertainment	Allow
Fashion & Beauty	Allow*
Finance & Investment	Allow
Food & Dining	Allow
Government	Allow
Health & Medicine	Allow
Hobbies & Recreation	Allow
Hosting Sites	Allow*
Infrastructure	Allow
Job Search & Career Development	Allow
Kid's Sites	Allow
Motor Vehicles	Allow
News	Allow
Philanthropic & Professional Organizations	Allow
Photo Searches	Allow
Politics	Allow
Real Estate	Allow
Reference	Allow
Religion	Allow
Search Engines	Allow
Shopping	Allow
Society & Culture	Allow
Sports	Allow
Streaming Media	Allow

Travel  
Uncategorized

Allow  
Allow\*

<b>Corresponding Websense Category (or categories)</b>	<b>Default Action</b>
Education > Cultural Institutions	Quota
Productivity > Message Boards & Forums	Block
Business & Economy	Permit
<i>(No equivalent. By default, requests sent to internal sites not monitored)</i>	Permit
Information Technology	Permit
Information Technology > Computer Security	Permit
Productivity > Pay-to-Surf	Block
User-Defined	Permit
Education > Educational Institutions	Permit
Education > Reference Materials	Permit
Entertainment	Quota
Society & Lifestyle	Quota
Business & Economy > Financial Data & Services	Quota
Productivity > Online Brokerage & Trading	Block
Society & Lifestyle > Restaurants & Dining	Quota
Government	Permit
Military	Permit
Health	Permit
Drugs > Prescribed Medications	Quota
Drugs > Supplements & Unregulated Compounds	Confirm
Society & Lifestyles > Hobbies	Quota
Information Technology > Web Hosting	Quota
Miscellaneous > Content Delivery Networks	Permit
Miscellaneous > Image Servers	Permit
Job Search	Block
Education > Education Materials	Permit
Vehicles	Quota
News & Media	Permit
News & Media > Alternative Journals	Quota
Social Organizations > Professional & Worker Organizations	Permit
Social Organizations > Service & Philanthropic Organizations	Permit
Social Organizations > Social & Affiliation Organizations	Permit
Bandwidth > Personal Network Storage & Backup	Block
Government > Political Organizations	Confirm
Shopping > Real Estate	Quota
Education > Reference Materials	Permit
Religion > Non-Traditional Religions & Occult	Quota
Religion > Traditional Religions	Quota
Information Technology > Search Engines & Portals	Permit
Shopping	Quota
Internet Auctions	Quota
Society & Lifestyles	Quota
Society & Lifestyles > Gay or Lesbian or Bisexual Interest	Quota
Sports	Quota
Sports > Sport Hunting & Gun Clubs	Quota
Bandwidth > Internet Radio & TV	Quota

Bandwidth > Internet Telephony  
Bandwidth > Streaming Media  
Travel  
Miscellaneous > Uncategorized

Quota  
Quota  
Quota  
Permit

**SMTP Inbound HOSTS****Ross/Portland/Munro**

\*.resultsmail.com  
\*. \*mailengine\*.com  
pc-live-care.com  
nahuysplyaga.ru  
onkagulertahul.com  
jfjfhfyhuqnbnciper.cz.cc  
\*@216-55-167-143.dedicated.abac.net  
livepc-care2010.com  
\*.dotnet-domain-web-hosting.net  
\*.hellenic-antiaging-academy.gr  
nationalsecurityorg.com  
\*.elektro-pfeffer.at  
\*.grupozeat.es  
live-pc-care2010.com  
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1297  
\*.sjasset.com  
zyns.com  
fburwellport.my03.com  
winecountryvineyards.info/demo/report.zip  
vulernubertuh.com  
freetemplatestoday.com/media/report.zip  
zulu705.server4you.de  
one-care-antivirus2010.com  
208.115.230.76  
bozo2011.webs.com  
\*.crocettamauro.it  
lorkajilopergul.com  
dot.us-state.org  
ertunaskodert.com  
zulu710.server4you.de  
vuleranumertu.com  
apport.myZ.info  
67.21.112.55

**SMTP Inbound SENDERS****Ross/Portland/Munro**

@gsamart.com  
investigationicegov@gmail.com  
cegentry2002@yahoo.com  
hxxp://worid-of-books.com/ur.php  
mehrads6t@mail.com  
toby.rubik@gmail.com  
bmail46@i24insight.com  
hxxp://alexblane.com/ur.php  
mail-google.dyndns.org  
aeko@hostmd.com  
hxxp://google-stats49.info/ur.php  
\*flewflyinghome.com  
sales@salesconvo.com  
dsullivan@washingtonpost.com  
ptkaiser.czechmission@gmail.com  
noreply@m10.myzamanamail.com  
fourseasons@e.fourseasons.com  
IAGConsulting@iag.biz  
\*@hoarty.com  
e444830555@exchange.1and1.co.uk  
noreply@message.zomp.nl  
capestonecounty.com  
system@bpa.gov  
anthony.vandivner@aaisolutions.com  
posta@tamgonder.com  
hxxp://tzv-stats.info/ur.php  
\*@chiediauto.it  
\*@scarsini.at  
\*@wallonieweb.be  
graham.prodger@durasystems.com  
homebanking@pnwfcu.org  
hunterjo41@nycdance.com  
us-bulletins@info.hp.com

\*.dewa.com.pl  
westernunion-mtcn[.]cz[.]cc  
\*.aesa-sa.com.ar  
64.95.64.197  
hxxp://zolotiyeyayca.ru/pusk2.exe  
bulkaserdat.com  
fmsalberta.com  
security-pc-care.com  
\*.enodivinus.com  
dertabuniokas.com  
cukerbuker.com  
:8080/index.php?pid=10  
tunabiolkert.com  
inationalsecurity.com  
www.x2c.dk/report.zip  
eitzxhcjw[.]cz[.]cc  
ubulertoniko.com  
\*cm.netteller.com  
fidessa.2tetra.com/report.zip  
winecountryvineyards.info/report.zip  
sadertubertug.com  
www.gnnet.co.kr\*  
networksecurityregistry.com  
\*server.birdfollow.com\*  
iertubalinos.com  
fburwell.my03.com  
avulkaqwerta.com  
internetsecurityinside.com  
bestpathsecurity.com  
live-pccare2010.com  
74.208.5.67  
securitypccare2010.com  
elloweksoqe.com  
osavoskalibom.com

mecaprojecto2012.biz.nf  
noreply@message.terebint.nl  
noreply@verizonwireless.com  
trenton.Price@liangtec.com  
f.skett@yahoo.com,  
hmedeiro@georgebrown.ca  
jill@clickback.com  
catherine02@blobomail.com  
iippgg-0014@hotmail.com  
posta@bultengonderim.com  
\*@academy.ca  
WrightMarketing@wrightusa.com  
obama.servehttp.com  
Chen.Ji@nnsa.srs.gov  
booking@culturalcenter.gov.ph  
\*happybehere.com  
\*@reeta4trading.\*  
nsi@dni.gov  
milena.lanza@labinco.com.co  
\*@gu.edu.au  
messengers.servebbs.com  
michael.a.marullo@infonetrix.ccsend.com  
webadmin@rhodes.edu  
news.canadatvsite.com  
laura@brasilelecom.net.br  
\*@sistemasgaitan.es  
www.zhitangvalve.com  
\*@minet.ca  
afn@fedweek.com  
maurice\_fleskens@hotmail.com  
adminqepbk@dhl.com  
Autodesk@ssprd7.net  
mail@infocommedia.info  
psalerts@email.workforce.com

quimeras.com.mx/report.zip  
www.educar-coop.com.ar/report.zip  
totalsecuritydirect.com  
abuhulertubae.com  
quimeras.com.mx/home/report.zip  
\*mp3.nilukco.com\*  
windowspc-care.com  
ddsk.se/images/report.zip  
my03.com  
security-pccare2010.com  
paidgeek.com/report.zip  
\*.bizsizanayasaolmaz.org  
\*.sk  
yoursecurityplus.com  
ionasderfulga.com  
getsecuritydirect.com  
\*service.birdfollow.com\*  
tanulertuval.com  
ponkaguilerda.com  
windows-pccare.com  
lorginavortag.com  
\*.ftp.halsat.sk  
\*.cinicolor.com.ar  
\*.enodivinus.com  
\*.dedicatedservers-hosting.com  
\*.alislam4all.com  
\*.aydintepeliler.com  
livepcantispyware.com  
https.join3com.com  
188.138.59.28  
pccareliveone.com  
celltechsecurity.com  
\*.ecdIxadress.altervista.org  
amostagorawe.com

\*@multidata.dk  
hxxp://alisa-carter.com/ur.php  
csolari.upeace@gmail.com  
info@sayma.es  
Neil.Price@puc.idaho.gov  
toyotalottocnpromo@gmail.com  
news@nextaq.com  
jessica.giles@carahsoft.com  
lynn.n.fisher@lmco.com  
jsimonetti.nsc@gmail.com  
dyfbh.youdontcare.com  
mb83706@att.net  
abolfazl-behzad@googlegroups.com  
noreply@fierceinc.com  
my@aaisolutions.com  
webmaster@halottlato.hu  
bijalk@garrisonenterprises.net  
hr@endtheclutter.com  
e.gz9@orange.fr  
www.nacha.org/news/newsDetail.cfm/RecentBusiness  
noreply@message.deltos.it  
info@blackdouglas.com.au  
maviegitim.2010@gmail.com  
up82673.hopto.org  
alaffay@mgl.com  
account.webcshosting.com  
Billgates.itsAOL.com  
\*@carms.ca  
noreply@message.somogyi.be  
sullivan01@kimo.com  
scatteredpicture@msn.com  
www.persh.org  
\*@integralcoaching.nl  
s.tomp@yahoo.com

\*.boschbitlis.com  
globalinformationsecurity.com  
\*.abac.net  
\*.alislam4all.com  
\*.aydintepeliler.com  
livepcantispyware.com  
https.join3com.com  
188.138.59.28  
pccareliveone.com  
celltechsecurity.com  
\*.ecdlexadness.altervista.org  
amostagorawe.com  
\*.boschbitlis.com  
globalinformationsecurity.com  
\*.abac.net  
tiesiog.puikiai.lt/report.zip  
myZ.info  
\*.ato3x85w.dev.pathcom.com  
nighthunter.ath.cx/report.zip  
kolabonganumba.com  
securityusaonline.com  
yoursecurityinfo.com  
\*.virustotal.com  
ulbrionaserty.com  
blacksecuritygroup.com  
www.racingfax.com  
securitypc-care.com  
kkojjors.net  
ertugaluholu.com  
nachausers-book.com  
\*.datasig.com.ar  
\*.restaurantlebed.com  
\*.uopinc.com  
\*.heregospel.com.br

noreply@message.weekendjeweg.nl  
dannice@gmail.com  
\*.nacha.org  
ermardugt@absamail.co.za  
janetkone17@yahoo.com.vn  
davia.homedns.org  
bmail46@i24insight.com  
babybarbara882@gmail.com  
tramirez@tdxpower.com  
ashley.hubler=mainstreamllc.com@cmail5.com  
pro@housing.go.ke  
mail.tvcaotw.com  
MRempel@nclud.k12.ca.us  
diamobi2000@yahoo.com  
log.mikeroark.com  
qhsnw2@gmail.com  
superaround.ns02.biz  
David.Avery@revenue.alabama.gov  
www.microsoft.acmetoy.com  
anil@thepixeldreams.com  
\*@fedconnect.net  
\*@vanloons.ca  
\*govntrip.com  
citicommercialcards.admin@citi.com  
Shopenya.com@firsatlari.biz  
bytehenge.com  
earthquake.japan@yahoo.com  
noreply@message.dbbm.unina.it  
no-reply@my4dx.com  
westryhungert@gmail.com  
jointcooper@yahoo.com  
\*govtrip.etravelsystem@rocketmail.com  
mingas.michel10@orange.fr  
bracken.hendricks09@gmail.com

direct.zyns.com  
ftp.join3com.com  
doe.cisconline.net  
207.174.21.159  
www.thepinkhouse.co.il/report.zip  
zolotiyeyayca.ru  
\*.ibcalvario.com.br  
ungahulertag.com  
qpoe.com  
lerkusaderfu.com  
hxxp://kkojjors.net/f/s.php  
bay0-omc2-s7.bay0.hotmail.com (bay0-omc2-s7.bay0.hotmail.com)  
rduilopesdae.com  
retailsecurityguide.com  
somashop.lv/report.zip  
hxxp://nahuysplyaga.ru/pusk2.exe  
wha.qpoe.com  
askkairatik.net/report.zip  
\*.cyrpainting.cl  
\*.aliviamos.com  
hxxp://cukerbuker.com/pusk2.exe  
\*stratfor.ushcime.com/  
google.vizvaz.com  
ftp.google.vizvaz.com  
antivirus-live-one1.com  
kaderbubioskal.com

mta8.brinkster.com  
Store.STOR.00.00.EN.ARV.KIT.CS.T01.SPT.00.EM@css.o  
jerrycompany@yandex.com  
bwood@woodduloherly.com  
k\_smat@yahoo.com  
francesco.presutti@gmail.com  
info@correo.cop.es  
global.faruk@gmail.com  
usgoodluck.com  
noreply@message.eskoleia.no  
ADMarketing=accessdata.com@mail60.us1.mcsv.net  
citrix@omnchnlbse.com  
noreply@message.derybarrette.ca  
etc-sales1@vip.163.com  
\*reetal4trading\*  
info@portalsf.com.br  
info@striker.ottawa.on.ca  
ground@fedex.com  
Aries.lee@dowell-cargo.com  
noreply@message.emergencyservice.hu  
duncansbay@hotmail.com  
Elizabeth.Donehue@srs.gov  
noreply@message.soneramail.nl  
sz\_ncec@vip.163.com  
ddrvlshr@aol.com  
info@sayma.es  
j.sprinkel@logixml.com  
oliver.davison@vg-energy.com  
webform@altium.com  
shahin\_bojari@googlegroups.com  
Marketing@micropowerdirect.com  
bsbhalla@indiagov.org  
info@cadaris.com.br  
stata.mail@esa.doc.gov

confirm@itp.es  
recruitmentmaritime@blumail.org  
noreply@message.happening.es  
scott.kaulf@gmail.com  
infoi2205@gmail.com  
iippgg-001@hotmail.com  
morales.p.david@gmail.com  
ftp.xmahome.ocry.com  
rsharon0@yahoo.com  
leadferretteam@leadferret.com  
for-drhays@bpa.gov  
ForefrontServerSecurity@SPCVM1182.com  
lcs@malaylegal.com  
\*@apold.ca  
m0rales.david@gmail.com  
qhsnw7@gmail.com  
user-zjg@tacoma.com  
thomsonreuters@icanmakeitbetter.com  
jo.aroma0701@googlemail.com  
info@ausbiotech.org  
jo.aroma0266@googlemail.com  
foreign@budgetconferences.com  
jenny.finley@ubc.ca  
\*Richard Morgan\*  
ds.mikeroark.com  
\*@estill.com.au  
hxxp://tadygus.com/ur.php  
hxxp://t6ryt56.info/ur.php  
wubshett@ethionet.et  
boeingasiarkshriver@rocketmail.com  
smartgrid-ci.com@mail35.us2.mcsv.net  
info@e.equifax.com  
azickefoose@multiview.com  
sales@aufeng-audio.com

info@nebrwesleyan.edu  
awoolf@crs.loc.gov  
1foxfiisa.com  
info@agreejp.com  
Jacobs Anti-Spam anti-spam@jacobs.com  
jo.aroma0264@googlemail.com  
info@qatar-airways.tk  
jennifer.hudson@jacobs.com  
jacobcolema5@gmail.com  
\*.reetal4trading.com  
Pjay4104@aol.com  
sistema.ticket@acens.com  
brian.knight=pragmaticworks.com@\*  
jky73@seohaeco.com  
canoedaily.com  
noreply@message.helpuremodel.com  
hxxp://stats-master88.info/ur.php  
The\_Villa\_Book@email-distribution.com  
enews@rodalenews.com  
\*@token.gov  
alere wellbeing@alere.com  
joaillerie.negoce@gmail.com  
jaime.loureiro@tjam.jus.br  
godzone2991@gmail.com  
jasonjoboco@yahoo.com  
events@eucievents.com  
\*@hurricanes.dk  
public-sector\_tech-pubs@comunycate.com  
GlowaceG@aol.com  
info@smartgrid-ci.com  
cenpangsjfq@sohu.com  
jacobkaruma2@gmail.com  
Jeanette.Kamar@nh.org.au  
jobs.shelloilcompanyuk@gmail.com

princessllu519@atayatirim.com.tr  
graphics@info.hp.com  
ajarez03@comcast.net  
tomg92539@gmail.com  
info@publicworksresource.net  
mikalaic@reseller10.hrwebservices.net  
mylife@mail.mylife.com  
smartgrid-ci.com@mail72.us2.mcsv.net  
addictingames.com  
sjtrp@ginfes.com.br  
noreply@message.corpusfitness.hu  
jackjame26@yahoo.com  
jennie@angelvisionmail.com  
confirm@novotemponet.com.br  
stbenson11@gmail.com  
rsvp@networkafterwork.com  
118-160-194-40.dynamic.hinet.net  
dontreplay@americanexpress.com  
jamie.burans@titus.cm  
jobs@energycentraljobs.com  
info@ayto-almansa.es  
symantec@omchbs.com  
noreply@message.videoheaven.com  
cuate2lalo@hotmail.com  
postmaster@comsatshosting.net  
anguishing73@roxore.com  
email@shop-onerewards.com  
snsarraaj@just.edu.jo  
\*@hecchiemagli.com  
walkervictoria62@yahoo.com  
member@messaging.zoosk.com  
lunasur5@yahoo.com  
messages-noreply@bounce.linkedin.com  
M.Slingerland@dordrecht.nl

\*.c3da.com  
gdrakademibulten@gmail.com  
roadhousegroup.com  
mail-googles.dyndns-mail.com  
ftp2.webcshosting.com  
emcweb.lucent.ddns.me.uk  
csware@compositesw.com  
THEODORAGUEST@GMAIL.COM  
leo.Sanchez@j-mdc.com  
ticket\_798@deltaa.com  
kingsleyagwor@umail.net  
service01.info@yahoo.com  
cpanelroundcube@cpanel1.servebyte.com  
lb@lewisbrothers.net  
mr.rodney\_s@yahoo.com.ph  
michoguna007@gmail.com  
mcnultysvise@yahoo.com  
megan.kunze@jacobs.com  
mail@seaservices-eg.com  
steve.jacyna@carahsoft.com  
sokeeffe@meritalk.com  
marycurto@yahoo.com  
Marketing1@skippingstonellc.com  
a.conteh@yahoo.com  
edeals@target.123dealz.net  
\*@strixchomutov.cz  
wag@spearmarketing.com  
mx@hksosphone.com  
gab.sgc@ifam.edu.br  
mfernandez@trisotech.com  
Jacobs Anti-Spam anti-spam@jacobs.com  
govntrip.com  
mantelpiecesfu3@roadhousegroup.com  
kurdyunatal@yahoo.com

support.id429@fedex.com  
www.microsoft.instanthq.com  
\*@spokeshave.ca  
editor@energynewswatch.com  
mrmsereda@yahoo.com.hk  
dolsgunss.com  
smith6@sbiinfo.in  
info@nokiamail.co.uk  
Member.Benefits@equifax.com  
Whitepapers@itnewsalert.com  
smtp.dynamiclink.ddns.us  
noreply@message.aydan.nl  
replies@nelsonpub.com  
training@ttoolboxes.com  
\*@riotinto.com  
mr.kenymicheal@consultant.com  
info=elecdata.com@mail2.us1.rsgsv.net  
\*capestonecounty.com  
domikstart.hopto.org  
tyler.cook@kmsfinancial.com  
DAVID@fyspeaker.com  
app@techvalidate.com  
mailmarketing@uygunfiyatagalaxys3.com  
mrsjuliaf@yahoo.com.ph  
\*@fxonline.cz  
Ungrand@n.org  
patrick11ngomezulu@gmail.com  
attorney.williammoore@lawfirm.co.uk  
test@stc-r.nl  
in.info\_off@yahoo.com.ph  
privacy@dynadot.com  
\*@216-55-167-143.dedicated.abac.net  
nada.golmie@gmail.com  
benefitsdirector@nationalpolicetraining.net

noreply@message.beachclubvroeger.nl  
Erik.Jurgutis@titus.com  
nguyen\_duc.kien@yahoo.com.vn  
dianemcirwa@hotmail.com  
info@correo.cop.es  
information@luv.southwest.com  
\*@bertassi.it  
hxxp://extra-service.info/ur.php  
christopher.m.sala@gmail.com  
hxxp://sol-stats.info/ur.php  
webmailadmin@info.org  
xxdd1@icloud.com  
mmacchiavelli@asuresoftware.com  
\*nacha\*  
email@email.cbpresearch.com  
\*@montecchio.it  
noreply@message.sierex.nl  
noreply@message.holborn.cz  
noreply@message.geldhalen.nl  
nelly@zeelandnet.n  
noreply@message.denada.dk  
varius.ultrices@yahoo.com  
jeffrey.hopkins@riotinto.com  
noreply@message.cafemaier.at  
sanshushaaj@blumail.org  
communication@merchantservices.bankofamerica.com  
Customer@mgl.com  
brocademarketing@brocade.marketingstudio.com  
efqf.xbirbb@infografias-3d.es  
adobe@carahsoft.com  
noreply@message.tots.be  
mail-by-google.dyndns.org  
noreply@message.typ82.info  
in.info\_off@yahoo.com.ph

TradeMagazines@omniclbse.com  
\*@olegus.com  
marketinginquiries@watchguard.com  
web.webcshosting.com  
contact.yahoodaily.com  
noreply@message.pilgaardroskilde.dk  
t\_iringo@aol.com  
google-mail.dyndns.org  
agoogole.in  
noreply@message.senato.it  
replies@earthnetworks.com  
sfield@dellsducks.com  
vanessa@vconsults.com  
vidaurri\_rj@yahoo.com  
boschser@m2g-24-59.spvservers.net  
inrc2010.japan@gmail.com  
safecheck.organiccrap.com  
2010rcp101@mnit.ac.in  
mobilmail-1.t-mobile.sk  
noreply@message.cabaretsex.nl  
bkoduah3@gmail.com  
e447040702@exchange.1and1.com  
noreply@message.de-heus.nl  
fu.chromeenter.com  
smartgrid-ci.com@mail40.us1.rsgsv.net  
hxxp://general-st.info/ur.php  
hxxp://defender-uqko.in  
yucqiyiadgbua@spyingshopper.com  
gallup@gallup3.com  
\*@modesto.com  
francjl@yahoo.com  
reparationsfh@buxrud.se  
hxxp://google-stats45.info/ur.php  
\*@rdbe.com.tr

karen.ahlnas@helsinki.fi  
ReachBase@clk20.com  
lightcap8@aol.com  
\*@limarex.be  
admin@textbusterlaunch.com  
\*western.utrack\*  
callmequeenanna@gmail.com  
info@weir.org  
\*@winlawwoodlot.ca  
noreply@message.firstlineconsulting.be  
cz88.net  
info@screvolutions.info  
riteaid@email2.riteaid.com  
resourcestosucceed.net  
rxensen@hotmail.com  
Haiti-Earthquake@state.gov  
lisa.white@metricstream.com  
rych67@gmail.com  
test@phantompoint.com  
\*@lebensberatung.it  
CLAIRE.LAJEUNESSE@dsb1.edu.on.ca  
Buffet80.itsaol.com  
rasol.r1@mail.com  
info@rdbe.com.tr  
alvinton.jetos.com  
\*@aevbvba.be  
hxxp://online-stats201.info/ur.php  
web.officc9011@nl.rogers.com  
admin@thefreebieteam.com  
lmgworks@gmail.com  
noreply@message.noyalutech.nl  
brian.adams@GovernmentTrainingInc.net  
citizensoldierpublicationgbd@smyrnamediagroup.com  
ReachBase@clk20.com

daniellagendo@aol.com  
phishguru.com  
s.charbonneau@titus.com  
terri.rehkop@sosintl.com  
mobilmail-1.eurotel.sk  
mebaker@degarmogroup.com  
duii1966@hotmail.com  
newsletter@digitalmediaonlineinc.com  
mcolo@meritmovingsystems.com  
google.vizvaz.com  
google.servebbs.com  
rodney@chollian.net  
ansme.com  
tv.tvcaotw.com  
fyfield@s423666193.onlinehome.us  
training@cust-mta5.dmsgs.com  
jennie@avglobalservices.com  
rsvp@networkafterwork.com  
regwork.exe  
george.friedman@stratfor.com  
info@nokia.com  
announcements@remi.com  
amyinger1@yahoo.com  
blackfriday@sti.com.mx  
tomwest@techcorr.com  
meritalk@meritalk.com  
news@ttoolboxes.com  
manuelgalatas@gmail.com  
sara.hosley@altium.com  
bwell1123@gmail.com  
johnlewis@metricstream.com  
tammy.carey0@gmail.com  
cafssdenise@aol.com  
crclark@adobe.com

noreply@message.apofruit.it  
info@meragiftmail.com  
louise@taylorectricutility.com  
responses@asg.com  
daisy88draws-1@yahoo.com.my  
cortiz@mail.arc.nasa.gov  
yh.offce036@hotmail.com  
\*@rallysport.hu  
bampohaffer117@adinet.com.uy  
\*@massaroassociati.it  
scasey@microstrategy.com  
support@cans.com.hk  
solutia-mxc.mail.eds.net  
service@.visa.com  
Sherry.Baker@hrsb.ns.ca  
info@waterlawresource.net  
spicyprincessfyp@gmail.com  
buffet.bbsindex.com  
BBochiardy@smynamedialogroup.com  
Sr [m.kozak@t-zones.sk]  
scottbowman@qualquantsignals.com  
albertstein.ddns.us  
noreply@message.desisti.it  
unitrendsteam@unitrends.com  
ftpem112@xs4all.nl  
support@bpa.gov  
duncansbay@hotmail.com  
autolix.tsai.essmtpautolix@autolix.tsai.es  
reply@mail.foodmanufacturing.com  
Rotaliana.com  
announcements@projectmanagementusa179.org  
supports@comcast.net  
imbasia@gmail.com  
coerulus\_01@yahoo.com

Willamette@xactmailb.com  
norbert.juellch@doe.gov  
info@ig.com.br  
manuelgalatas\_imf@yeah.net  
pleiadi@hotellepleiadi.it  
\*@laposte.be  
chris.eager91@gmail.com  
free2.77169.net  
noreply@message.aanvallen.nl  
susanc@custardconsulting.com  
talk-noreply@google.com  
lxksolutions@lexmark.com  
root@w862.widhost.net  
chrleslundy@aol.com  
info@passarinbebidas.com.br  
claudine.potvin@ubc.ca  
tpockrus@multiview.com  
newsletters@advantagecontinuingeducationseminars.i  
mbelively@aol.com  
mail@infonetweb.info  
solutions@response.basware.com  
alt.c3da.com  
benignwgps108@bmatter.com  
info@ical.com.br  
\*@nacha.org  
mr.soolee@yahoo.com.cn  
smtp.c3da.com  
tyjilcorp@yahoo.com  
info@iconstituentpublicsector.com  
tham@himalayancomponents.com  
technology.specials@howardcomputers.com  
training@cust-mta5.dmsgs.com  
citrix@omnibse.com  
www3.mikeroark.com

\*@nervioplastics.be  
ojeradagdagan@yahoo.com  
rocket4ks@yahoo.com  
TIMRON@SYMPATICO.CA  
serrato.christy@gmail.com  
dyfbh.passas.us  
SalesOps@WatchGuard.com  
easytrustfinancialhome1@yahoo.com  
\*@farcama.com  
\*@striker.ottawa.on.ca  
kim.lukes@yahoo.com  
tatiana20@orange.fr  
hxxp://stats-master99.info/ur.php  
ADMarketing=accessdata.com@mail83.us4.mcsv.net  
csiswork@aol.com  
mohamadreza.f3@mail.com  
\*@elap.es  
fbdbscrub12.att-mail.com  
redi5motorsinc@hotmail.com  
\*@simulator.be  
administrator@bpa.gov  
sine.sn30428@gmail.com  
tracking@usps.com  
\*@\*.token.gov  
Blizzcon.sexxy.biz  
resourcestosucceed.net training@resourcestosucceed.  
FCW@1105Info.com  
a@rcctvm.org  
felberthom@aol.com  
postmaster@ns4.nest.vn.ua  
overseas@fakt.com.pk  
sayersas@unhabitat.org  
rmi@utep.edu  
paulf@sanspot.com

info@recruitment.com  
monadas9@gmail.com  
info@lsilsnews.com  
afnewcastl@yahoo.com  
acquisitionofestate7@gmail.com  
fmclane@webroot.com  
manohar\_lal@eroads.in  
c3da.com  
tarun.mahandru@pearllinguistics.com  
websm27110@gmail.com  
OHS@1105Info.com  
events@euci-events.com  
egm@ciudad.com.ar  
williammoore@lawfirm.co.uk  
fluke@e.fluke.com  
google-mail.dyndns-web.com  
emarsh@protechtraining.com  
hxxp://stats-master111.info/ur.php  
corp.c3da.com  
brian.knight=pragmaticworks.com@mail22.wdc01.mcc  
yvonne@hlb.com.sg  
smartgrid-ci.com@mail41.us1.mcsv.net  
noreply@message.obszeester.nl  
noreply@message.ansa.no  
rsandstrompdx@yahoo.com  
ur-460@coloradosprings.com  
\*@orf.at  
fbNOREPLY@myfanbox.com  
\*@PerformanceTrainingSolutions.com  
znqsttry3v@hkip1216.u9bbs.com  
subscribe@cathstan.org  
\*@alerts2.alertlink.com  
flyfisher611@netzero.net  
294.QD@riverside.com

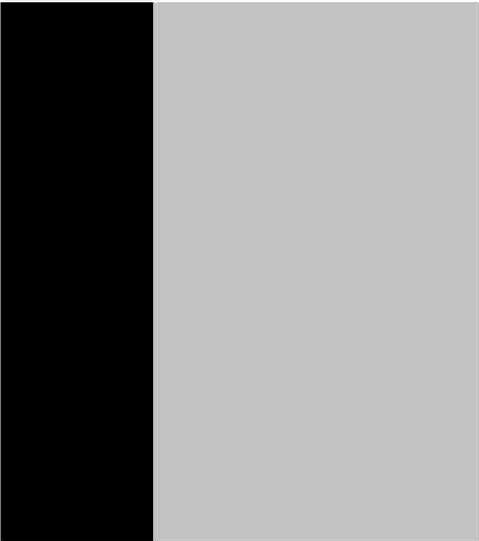
34.def45@gmail.com  
lhx@smartbrief.com  
\*@demetal.nl  
podiumsv92@ropsalons.com  
email@1800gotjunk.messages3.com  
smartgrid-ci.com@mail16.us4.mcsv.net  
\*.wikileaks.org  
noreply@message.victumigcn.nl  
\*@oosteromopleidingen.nl  
daniel.hitchcock@ymail.com  
info=elecdata.com@mail278.us2.mcsv.net  
536.ssx@newyork.com  
no-reply@skillpagesmail.com  
info=elecdata.com@mail345.us3.mcdlv.net  
hxxp://google-stats50.info/ur.php  
noreply@message.lerares.nl  
corsello\_michael@bah.com  
info@weir.org  
ashley@hiras-fashions.com  
683-uhr@tucson.com  
clinkousr@yahoo.com  
\*@acif.org.br  
info@technologytransfertactics.com  
\*@kjc.fi  
DMacallum@ezloader.com  
ameena@aol.com  
hxxp://lizamoon.com/ur.php  
promoreplies@freetrademagazines.com  
ecdirect-daily@energycentral.com  
claudia.huffman@afgimail.com  
www.microsoft.proxydns.com  
customerservice@lorman.com  
broadcaster.ss.marketing@gmail.com  
info@famedmedikal.com

user.afk@greensboro.com  
blackfriday@\*  
confirm@practice.com.br  
aurelie.laffay@alpsp.org  
fcpra1@serv01.siteground221.com  
info@melbournewater.com.au  
casowens27@aol.com  
\*@hightechnologyseminars.\*  
smartstream@itsjss.com  
tjpsstriker11@comcast.net  
skim.service@yahoo.com  
selma@ibb.unesp.br  
Pratik.chavan@harbingergroup.com  
mail@techwebnet.info  
bodzye@email.arizona.edu  
mailbot@yahoo.com  
www.insiso.co.uk  
pwelbeck080@gmail.com  
\*@newdevices.com  
lmengineeringcontractor@gmail.com  
info@msn.co.uk  
bampomah@cantv.net  
Brian.adams@GTITrainingSolutions.com  
cho@showgard.com  
189104132239.user.veloxzone.com.br  
larryfanger@aol.com  
dyfbh.longmusic.com  
noreply@notifications.skype.com  
stefan.koopman@asdreports.com  
happybehere.com  
cometoway.org  
info@salesforce.com  
Hr2013@incomesecurities.com  
unfitsm@solutia.com

landsend@email.landsend.com  
gmail.dyndns.tv  
dascoli@bnl.gov  
Blizzcon.sexidude.com  
\*@lyngstol.no  
Ellswerthpmr278@yahoo.com  
info@federalemmployeeadvocates.org  
usaidgov@gmail.com  
ventas10@capacitaciondevededores.com  
candon@chowking.net  
dh.654@montgomery.com  
susanc@custardconsulting.com  
Newsletters@parrishtaylor.com  
hxxp://milapop.com/ur.php  
football.dynamiclink.ddns.us  
etap.seminars@etap.com  
EMPublications@exchangemonitor.com  
janett.serrano@gmail.com  
mail@mediainfocom.info  
Montoya@team-working.info  
www.WikiLeaks.org  
bjohn@pacificu.edu  
notification@123greetings.com  
\*skypehelpcn.com  
\*yahomail.net  
\*ieee.boeing-job.com  
\*engage.intelfox.com  
admin@enterpriseguide.com  
\*spacefoundation.org  
\*369p.mail-signin.com  
\*bm1k8.4pu.com  
\*cti.moobesring.com  
\*domcon.microtrendsoft.com  
news.canoedaily.com

\*engage.intelfox.com  
\*funny.greenitenergy.com  
\*i0i0i.3322.org  
\*ieee.boeing-job.com  
\*krjregh.sacreeflame.com  
dontreply@intuit.com  
\*lol.dns-lookup.us  
\*lywja.healthsvsolu.com  
\*matrix.linkerservices.com  
\*mx.dns221.com  
hxxp://eva-marine.info/ur.php  
\*piping.no-ip.org  
\*ru.pad62.com  
\*stmp.allshell.net  
\*support.icoredb.com  
\*svr01.passport.serveuser.com  
\*ukupdate.masteradvz.com  
training@resourcestosucceed.net  
\*update.mysql1.net  
\*update.updates.mefound.com  
\*update1.mysql1.net  
seminars@cvent.com  
\*update3.effers.com  
\*updatedns.itemdb.com  
\*updatedns.serveuser.com  
training@resourcestosucceed.net  
\*update.mysql1.net  
\*update.updates.mefound.com  
\*update1.mysql1.net  
seminars@cvent.com  
\*update3.effers.com  
\*updatedns.itemdb.com  
\*updatedns.serveuser.com  
humanright@uconn.edu

anonymousbpa@gmail.com  
jliverpool@exagrid.com  
info@i360gov.com  
\*@letterstyl.be  
yahoodaily.com  
\*@gemeenschapsonderwijs.be  
flewflyinghome.com  
jademason.com  
good.mincesur.com  
jwessinger@emergent360.com  
conferences@powermarketers.com  
wilfredredew@net.hr  
\*@scripto.be  
hxxp://google-server43.info/ur.php  
pratik.chavan@harbingerproducts.com]  
acton@natsem.com  
email@employers.messages5.com  
tracking@ups.com  
craigbabb@afgimail.com  
juheeki@ygone.com  
noreply@message.regionliberec.cz  
noreply@message.excite.it  
\*@topaze.be  
prc.dynamiclink.ddns.us  
pahodges@bpa.gov  
\*@frialto.com.br  
\*@nyberg.com  
mrmuhadikabore1@yahoo.com  
john@transhorsa.org  
\*@nocigi.hu  
scaircrow16@yahoo.com  
tickets@delta.com  
user.ihd@minneapolis.com  
contact@mindswaysinfo.us



mail@infomediacom.info  
govtrip.etravelsystem@rocketmail.com  
hxxp://agasi-story.info/ur.php  
www.yhao.mrface.com  
brian.adams@GovernmentTrainingCourses.net  
sherilawrence@gmail.com  
ashley.hubler=mainstreamllc.com@cmail2.com  
bupasi.9966.org  
chris.bush@srs.gov  
mmiller@ains.com  
seminar@targetedconferences.net  
posta@postaduyuru.com  
western.utrack@gmail.com  
\*@sauber.nl

NewsID/207

ne.microsoft.com

n

com

net

ilv.net

Case	Employee Name	Summary	Status	Assigned To	Date/Time Created	Target Close Date	Closed Date	Empl ID	Department	Location	Physical Location	Priority	Provider Group	Created By	Asset Tag
1772734	Ex 6	UNBLOCK: BPA Flickr Website blocked (again). Need fixed for BPA Connection	Closed - Resolved	Ex 6	01/25/2013 3:34PM	1/25/2013	01/29/2013 4:06PM	3612	Ex 6	Portland	Ex 6	Medium	Firewall	DDD9506	
1751599		Website blocked	Closed - Resolved		11/14/2012 11:10AM	12/14/2012	11/14/2012 11:10AM	9378		Vancouver		Medium	Help Desk	CDC3112	
1705720		INFO: Website blocked - need to purchase software	Closed - Resolved		06/06/2012 3:05PM	7/6/2012	06/06/2012 3:06PM	8443		Portland		Low	Help Desk	EER8604	
1462681		4161: Corps website blocked by proxy	Closed - Resolved		06/30/2009 3:44PM	7/30/2009	07/06/2009 2:59PM	4954		Portland		Medium	Operations Application Delivery	TOM5727	
1275392		UNBLOCK: Why is the United Air Lines website blocked while the Alaska Air Lines	Closed - Resolved		08/15/2007 7:50AM		08/15/2007 2:26PM	2377		Portland		Medium	Cyber Security	CAR7257	
1265305		Info: Website blocked	Closed - Resolved		07/11/2007 1:51PM		07/11/2007 2:00PM	2959		Goshen		Medium	Help Desk	DMM1676	
1235995		Cyber: Website blocked, see notes	Closed - Resolved		03/27/2007 9:40AM		03/27/2007 10:35AM	792		Seattle		High	Cyber Security	DMM1676	
1230400		Red Triangle:Wants to have someone to contact her regarding website blocking.	Closed - Resolved		03/08/2007 6:05AM		03/09/2007 10:37AM	4429		Portland		Medium	Cyber Security	EAM5221	
1227251		Cyber: Website Blocked, see notes	Closed - Resolved		02/26/2007 3:45PM		02/27/2007 8:55AM	675		Idaho Falls		High	Cyber Security	DMM1676	
1121025		Government website blocked	Closed - Resolved		11/30/2005 5:14PM		12/21/2005 4:36PM	4640		Vancouver		Medium	UNIX Support	JAC3836	

Case	Employee Name	Summary	Status	Assigned To	Date/Time Created	Target Close Date	Closed Date	Empl ID	Department	Location	Physical Location	Priority	Provider Group	Created By	Asset Tag
1669471	Ex 6	WEBSITE UNBLOCK; FW: Unblock request	Closed - Duplicate	Ex 6	01/13/2012 11:21AM	1/20/2012	01/18/2012 10:57AM	3190	Ex 6	Portland	Ex 6	Low	Cyber Security	TDK1562	
1698559		INFO: Website unblock request	Closed - Resolved		05/09/2012 10:28AM	5/9/2012	05/09/2012 10:55AM	3244		Portland		Low	Help Desk	TDK1562	
1698760		INFO: Website unblock	Closed - Resolved		05/09/2012 5:37PM	5/11/2012	05/09/2012 5:37PM	2117		Portland		Low	Help Desk	TDK1562	
1707187		INFO: question on how to get website unblocked	Closed - Resolved		06/12/2012 3:48PM	7/12/2012	06/12/2012 3:50PM	3771		Portland		Low	Help Desk	CDC3112	
1708670		INFO: how to get website unblocked.	Closed - Resolved		06/18/2012 2:32PM	7/18/2012	06/18/2012 2:32PM	5068		Portland		Low	Help Desk	CDC3112	
1708889		INFO: how to request a website unblock	Closed - Resolved		06/19/2012 9:49AM	7/19/2012	06/19/2012 9:55AM	5260		Portland		Low	Help Desk	RAP2920	
1709035		INFO: User wants to know how to get a website unblocked	Closed - Resolved		06/19/2012 1:06PM	7/19/2012	06/19/2012 1:07PM	3115		Portland		Low	Help Desk	EER8604	
1710334		WEBSITE Unblock Request: approved by Marvin Whitmore	Closed - Resolved		06/22/2012 10:45AM	7/22/2012	06/25/2012 10:52AM	402		Portland		Medium	Firewall	CDC3112	
1710491		INFO: How do I request a website unblock	Closed - Resolved		06/22/2012 3:02PM	7/22/2012	06/22/2012 3:03PM	3535		Vancouver		Low	Help Desk	RAP2920	
1711822		INFO: how to get website unblocked.	Closed - Resolved		06/27/2012 5:49PM	7/27/2012	06/27/2012 5:57PM	11913		Portland		Low	Help Desk	CDC3112	
1712952		WEBSITE UNBLOCK REQUEST: Approved by David Pease	Closed - Resolved		07/02/2012 4:47PM	8/1/2012	09/04/2012 7:49AM	10515		Portland		Medium	Cyber Security	CDC3112	
1714140		WEBSITE UNBLOCK REQUEST: Approved by David Pease	Closed - Resolved		07/09/2012 12:38PM	7/9/2012	07/09/2012 1:02PM	10515		Portland		Medium	Server Access Control	JDE0766	
1724299		INFO: How do I get a website unblocked?	Closed - Resolved		08/14/2012 10:54AM	9/13/2012	08/14/2012 10:55AM	2134		Portland		Low	Help Desk	RAP2920	
1729671		INFO: How do I get this website unblocked?	Closed - Resolved		08/31/2012 9:23AM	9/30/2012	08/31/2012 9:23AM	4633		Portland		Low	Help Desk	RAP2920	
1731784		INFO: how to get website unblocked	Closed - Resolved		09/10/2012 10:45AM	10/10/2012	09/10/2012 10:46AM	10094		Olympia		Low	Help Desk	CDC3112	
1733186		INFO: How do I get a website unblocked	Closed - Resolved		09/13/2012 10:01AM	10/13/2012	09/13/2012 10:01AM	10544		Vancouver		Low	Help Desk	RAP2920	
1733945		INFO: How do I get a website unblocked?	Closed - Resolved		09/17/2012 8:30AM	10/17/2012	09/17/2012 8:30AM	1669		Portland		Low	Help Desk	RAP2920	
1736826		INFO: How do I get a website unblocked?	Closed - Resolved		09/25/2012 11:14AM	10/25/2012	09/25/2012 11:15AM	4964		Portland		Low	Help Desk	RAP2920	
1737275		Request for Website Unblock	Closed - Resolved		09/26/2012 11:02AM	9/27/2012	09/27/2012 9:40AM	4383		Portland		Medium	Server Access Control	AAN6317	
1737555		INFO: How to have website unblocked for GIC Simulator Program on 4000264	Closed - Resolved		09/27/2012 8:58AM	10/27/2012	09/27/2012 9:05AM	11838		Vancouver		Low	Help Desk	MLB4670	4000264
1737581	Request for Website Unblock	Closed - Resolved	09/27/2012 9:38AM	9/27/2012	09/27/2012 9:40AM	4910	Vancouver	Medium	Server Access Control	KDJ0861					