BPA Policy 230-1

Monitoring and Recording Conversations

Table of Contents

1. Purpose & Background

To establish requirements, assign responsibilities, and provide guidance regarding the practice of recording and monitoring certain business conversations.

In addition, sets forth BPA policy on the general prohibition against the procurement, installation, or use of wiretapping, eavesdropping, or recording devices for any other purpose other than those listed in section 230-1.5 of this document.

2. Policy Owner

The Chief Operations Officer, working through the Governance and Compliance office, in collaboration with BPA's Chief Security and Continuity Officer provides overall management of this policy and is responsible for monitoring, evaluating, and proposing revisions to this policy.

3. Applicability

All BPA Employees

4. Terms & Definitions

A. Eavesdropping: Interception, through use of electronic equipment, of a conversation involving one or more individuals.

B. Wiretapping: The direct or inductive coupling of an electronic device to any line, or system, transmitting communications.

C. Recording: The use of a tape recorder, or similar device, to record the oral communication occurring on communication systems, or in meetings. This includes the use of portable, handheld recording devices which can be held up to the earpiece of a telephone.

D. Unauthorized Recording Device: An electronic device used to record conversations, meeting proceedings, confidential discussions, or any other private matter, without the knowledge or consent of the participants involved.

E. Wiretapping or Eavesdropping Device: An electronic device designed primarily to intercept communications.

5. Policy

It is BPA's policy to limit the recording, wiretapping or eavesdropping on all communications systems, including commercial telephone, Dial Automatic Telephone Switching (DATS), UHF/VHF radio, and cell phone transmissions, and to record and retain all commercial data recordings and emails directly related to ONLY the following types of business transactions

A. Power generation asset management (preschedule, real-time, transfer and after-the-fact) and dispatching;

B. Transmission system dispatching, reliability and maintenance operations;

C. Transmission sales and marketing transactions for requesting, managing, and scheduling transmission and ancillary service;

D. BPA Power Services Bulk Hub power and transmission purchases and sales operations;

E. Information Technology Help Desk conversations;

F. Criminal investigations;

G. All BPA employee meetings; and

H. BPA-hosted public meetings

BPA informs all parties engaged in the recording of conversations that occur via commercial telephone, Dial Automatic Telephone Switching (DATS), UHF/VHF radio, and cell phone transmissions, directly related to the business transactions listed in items A through D of section 230-1.5, by indicating that such conversations are being recorded by the presences of an audible tone at the beginning and throughout the recorded conversation. In addition, notification of BPA's policy on monitoring and recording conversations is provided on the individual web sites for BPA's Power and Transmission organizations and on bpa.gov.

It is also BPA's policy to prohibit the recording, wiretapping or eavesdropping on all communications systems, including commercial telephone, Dial Automatic Telephone Switching (DATS), UHF/VHF radio, and cell phone transmissions for any purpose other than those business transactions outlined in this policy.

The requisition of any equipment that enables recording, wiretapping or eavesdropping on communications systems other than for those business operations purposes listed in this policy is prohibited.

6. Policy Exceptions

A. Recording devices used for dictation or for the overt recording of all employee or public meeting proceedings or events.

B. Recording devices used in accordance with the terms and conditions of a Reasonable Accommodations Agreement. Information recorded under this exception must be secured in an appropriate manner.

7. Responsibilities

A. All BPA employees are responsible for immediately reporting to the BPA Manager for Security and Continuity of Operations, any suspicion of prohibited recording, wiretapping, or eavesdropping devices or practices. All BPA employees and contract personnel should not remove, disconnect, or tamper with any such suspected devices.

B. BPA Supervisors and managers are responsible for all activities noted in section 230-1.7 A., and for insuring that employees do not requisition or use prohibited recording, wiretapping or eavesdropping devices or practices.

C. The Chief Supply Chain Officer and Supply Chain managers are responsible for assuring that their staff are aware of BPA's policy which prohibits procurement of eavesdropping and wiretapping devices for uses not directly related to the BPA business operations functions outlined in section 230-1.5 of this document. Recording devices such as those used for dictation, or for the recording of meeting proceedings, may be procured with appropriate management approval.

D. The Manager of Transmission Systems Operations is responsible for developing and issuing directives and/or training on the implementation of this policy internal to his/her organization.

E. The Vice President of Transmission Marketing and Sales is responsible for developing and issuing directives and/or training on the implementation of this policy internal to his/her organization.

F. The Vice President for Power Services Bulk Marketing is responsible for developing and issuing directives and/or training on the implementation of this policy internal to his/her organization.

G. The Vice President for Generation Asset Management is responsible for developing and issuing directives and/or training on the implementation of this policy internal to his/her organization.

H. The Chief Security and Continuity Officer is responsible for:

1. Securing necessary reviews, approvals and/or authorizations from appropriate law enforcement authorities prior to granting approval for the use of sanctioned wiretapping, recording, or eavesdropping equipment in the event of a criminal investigation.

2. Notifying the Department of Energy (DOE) Director, Office of Safeguards and Security, and the local FBI office if any unauthorized recording, wiretapping or eavesdropping devices are discovered.

3. Forwarding a report, within 12 hours after the discovery of such a device, to the DOE Director, Office of Safeguards and Security, detailing:

a. the circumstances of the discovery of the unauthorized recording, wiretapping or eavesdropping device;

b. the location of the device;

c. BPA management notification;

d. FBI notification;

e. advice received from the FBI;

f. Federal Protective Service (FPS) notification when involving GSA-owned buildings and or facilities; and

g. other actions taken.

4. Advising the DOE Director, Office of Safeguards and Security, prior to the attachment or inductive coupling to telephone or teletype lines, of any devices capable of recording conversations or telephone numbers or otherwise secretly intercepting communications not normally used in routine transmission system dispatching, switching, and system maintenance operations, or in BPA power purchase and sales operations.

8. Standards & Procedures

All BPA employees and contract personnel are strictly prohibited from using any government-owned or personal recording and/or eavesdropping device on any communications system, internal or external, unless it is authorized as being directly related to the business operations functions outlined in section 230-1.5 of this document.

9. Performance & Monitoring

This policy will be regularly monitored for compliance and meeting the standards outlined in the various authorities listed below.

10. Authorities & References

A. Federal Law:

1. The Fourth Amendment
2. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 – 18 U.S.C. §2511. As Amended by Electronic Communications Privacy Act of 1986
3. Stored Communications Act of 1986 – 18 U.S.C. § 2701
4. Privacy Act of 1974 – 5 U.S.C. §552a
5. North American Energy Reliability Corporation (NERC) Standard INT-003-3, November 5, 2009 http://www.nerc.com/files/INT-003-3.pdf.
6. NERC Standard COM-001-1.1, May 13, 2009 http://www.nerc.com/files/COM-001-1_1.pdf.

B. State Law:

1. California – Cal. Penal § 630-38
2. Idaho – Idaho Code Ann. §18-6702
3. Montana – Mont. Code. Ann. § 45-8-213 (2009)
4. Nevada – Nev. Rev. Stat. §200.620 (2009)
   a. Nev. Rev. Stat. Ann. § 707.900
   b. See Lane v. Allstate Insurance Company, 969 P.2d 938, 940 (Nev. 1998) for Nevada Supreme Court interpretation of statute

5. Oregon – Or. Rev. Stat. §165.540

6. Utah – Utah Code Ann. §77-23a-4

   a. Utah Code Ann. §76-9-403

7. Washington – RCW §9.73.030

8. Wyoming – Wyo. Stat. §7-3-702 (2009)

C. International – Canada

1. Federal – Personal Information Protection and Electronic Documents Act

2. Provincial – Personal Information Protection Act (British Columbia)

11. Review

This policy is scheduled for review in 2019.

12. Revision History

Version	Issue Date	Description of Change
2	12/9/2014	Re-formatted into new template.
2.2	10/29/2018	Current template