BPA Policy 230-1

Monitoring and Recording Business Conversations

Table of Contents

1. Purpose & Background

This policy is to establish requirements, assign responsibilities, and provide guidance regarding the practice of recording and monitoring conversations and meetings on BPA property or during official activities.

It also sets forth the general prohibition against the procurement, installation, or use of wiretapping, eavesdropping, or recording (audio and/or video) devices for any purpose other than those authorized in section 230.5.c-d of this document.

2. Policy Owner

The Chief Administrative 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

This policy applies to all activities on BPA property or while performing official BPA activities.

4. Terms & Definitions

A. **Eavesdropping**: Secretly or stealthily recording a conversation, meeting or other activity.

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

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

D. **Wiretapping or Eavesdropping Device**: An electronic device designed primarily to secretly or stealthily record communications.

5. Policy

A. **Unauthorized Monitoring or Recording**: Recording or monitoring conversations, meetings or other activity by means of any recording or listening method, or authorizing or permitting others under their supervisory control to monitor or record others by the use of any device or method is unauthorized except:

1. As authorized by law, regulation or policy;

2. When an appropriate management official authorizes recording, and all parties are notified in advance; or
3. In the context of a telephone/digital call center or similar operations (i.e. energy trade centers). In such situations, supervisors may monitor or record conversations for evaluating employee performance or the maintenance of business records with proper notice to all parties to the communication.

B. **Recordings**: BPA prohibits video or audio recordings, wiretapping or eavesdropping using any device (voice, video, image, or otherwise) for any purpose other than those business activities outlined in this policy. The information owner of recordings is the office of record. All recordings shall be stored and retained in accordance with records management requirements.

C. **Limited authorization to make recordings related to business transactions**: BPA permits recordings related to the following types of business transactions and operations:
1. BPA Power Services Generation: asset management and dispatching;
2. BPA Power Services Bulk Hub: power and transmission purchases and sales transactions;
3. Transmission system dispatching, reliability, and maintenance operations; and
4. Transmission sales and marketing transactions for requesting, managing, and scheduling transmission and ancillary service.

D. **Limited authorization to record other activities at BPA**: BPA permits recordings in a limited number of non-transactional situations. Requests that are not addressed below shall be preapproved by the organization's supervisor or manager. Only the following types of actives are authorized for recordings:
1. Information Technology Help Desk calls.
2. Criminal or administrative investigations;
3. Internal meetings by the Administrator for all employees.
4. The monthly BPA Manager Update meeting;
5. BPA meetings related to decisions on Federal Columbia River Power System operations;
6. BPA-hosted public events;
7. Public involvement meetings;
8. Customer meetings; and

9. Emergency response activities as described in the Comprehensive Emergency Management System Guide.

E. **Conversations and meetings that are being recorded must ensure all parties are aware and informed of the recording**: Prior to any recording activity, including those authorized by this policy, all participants shall be informed that the activity will be recorded.

F. **Purchasing Equipment that enables Recording**: BPA prohibits the requisition of any equipment that is specifically purchased for recording, wiretapping or eavesdropping on communications systems other than for those business operations listed in this policy.

6. Policy Exceptions

A. Recording within the terms and conditions of a Reasonable Accommodations Agreement. Information recorded under this exception is the responsibility of the recording employee and must be protected in accordance with Information Security safeguards. Recordings that contain Personally Identifiable Information must be protected according to the safeguards required for controlled unclassified information for privacy related information.

B. Recording during incident command and emergency response situations.

7. Responsibilities

A. **Employees**: All BPA employees are responsible for immediately reporting any suspicion of prohibited recording or practices through use of any medium to their supervisor and/or BPA's Chief Security Officer. The BPA workforce should not remove, disconnect, or tamper with any such suspected devices.

B. **Supervisors and Managers**: BPA supervisors and managers shall ensure staff in their organization are aware of this policy, respond in a timely manner for activities noted in section 230.5.d, and ensure that employees do not requisition or use prohibited recording devices or practices as noted in section 5 of this policy.

C. **Chief Supply Chain Officer**: BPA's Chief Supply Chain Officer shall have published controls around the purchasing of recording devices and ensures Supply Chain managers are knowledgeable about BPA's policy prohibiting procurement of recording devices for uses not directly related to the BPA business operations functions outlined in section 230.5.c-d of this document.

D. **Chief Information Officer**: BPA's Chief Information Officer shall have controls around the purchasing and implementation of technology and software tools that have recording capability and ensure they are compliant with this policy.

E. **Chief Security and Continuity Officer**: BPA's Chief Security and Continuity Officer is responsible for:

1. Notifying the BPA Privacy Office if any unauthorized recording devices are discovered.
2. Notifying Federal Protective Service of any unauthorized recording device within any BPA facility or motor vehicle.
3. Tracking incidents in Security's Incident Reporting System for the official record.

8. Standards & Procedures

There are no general standards or procedures for this policy.

9. Performance & Monitoring

Compliance with this policy will be tracked in the compliance tracking mechanisms.

10. Authorities & References

A. Federal Law:

1. 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.
2. Stored Communications Act of 1986 – 18 U.S.C. § 2701.
3. Privacy Act of 1974 – 5 U.S.C. §552a.

B. Department of Energy Guide 151.1-B, Comprehensive Emergency Management System Guide, 4.4.5.2. Command, Control, and Communications Equipment.

11. Review

This policy is reviewed every three (3) years for errors, omissions and clarity by the Chief Security and Continuity Officer.

12. Revision History

Version Number	Issue Date	Brief Description of Change or Review
1.0	10/29/2018	Installed in current template
2.0	10/18/2024	Edited language as per OGC to resolve comments and edits from various BPA organizations