TELEPHONE SECURITY

ISSP-26-0410

1. **SUBJECT:** OPIC telephony resources are subject to the same security requirements and protections as other information resources.
2. **SCOPE:** This policy governs the use of telephones, modems, PBXs, and other telephony resources at OPIC.
3. **DESCRIPTION:** Telephone services are intended to support the objectives and operations of OPIC, and are critical to fulfilling OPIC's mission. These telephony resources are vulnerable to a variety of security threats and should be granted the same protection as other information resources.
4. **PROCEDURES & GUIDELINES:**

   (a) When using the OPIC phone system or OPIC-issued cellular phones, users should adhere to the following guidelines to protect the information communicated:

   (1) Understand that there should be no expectation of privacy when using these resources.

   - OPIC may audit use of these resources.
   - It is possible for third parties to tap or redirect phone calls outside of OPIC.

   (2) No sensitive data should ever be discussed over a mobile phone because of the ease of intercepting such communications.

   (3) Make sure that the person on the other end of the conversation is who they say they are. Do not give out sensitive information (including agency credit card information) unless you are sure of the person on the other end of the line.

   (4) Be cautious when discussing sensitive information that the conversation cannot be overheard by unauthorized persons (such as visitors to OPIC). Minimize use of speakerphone.

   (5) Obey relevant laws regarding the recording of phone conversations, including informing the other party that you are recording.

   (6) Follow OPIC's Acceptable Use policy in using phone resources, just as you would with email or other information resources.

   (b) The agency PBX and other critical telephony components must be protected:

   (1) This equipment should be stored in a secure, environmentally controlled location in accordance with OPIC physical security policy.

   (2) Telephony equipment is subject to the same security policies as other computer equipment, including Access Control, Change Control, Auditing, Patch Management, Server Security, Network Security, etc.

(3) Additional security threats and vulnerabilities applicable to telephony equipment must be analyzed and mitigated commensurate with the levels of risk, and criticality/sensitivity of those resources.

(c) Modems or other telephony equipment may not be installed without the explicit approval of the appropriate official (*e.g.*, OPIC Telecommunications Officer for telephone equipment, or Director of Technical Services for modems and related telephony equipment).

(d) Analog Phone Lines - As a rule, the following applies to requests for fax and analog lines:

(1) Fax lines are to be approved for departmental use only. No fax lines will be installed for personal use.

(2) Fax machines must be placed in centralized administrative areas designated for departmental use, and away from other computer equipment.

(3) A computer that is capable of making a fax connection is not to be allowed to use an analog line for this purpose.

(4) Waivers for the preceding policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and security posture of the request. If a waiver is provided, the use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized user to enforce at all times:

- The fax line is used solely as specified in the request.
- Only persons authorized to use the line have access to it.
- When not in use, the line is to be physically disconnected from the computer.
- The line will be used solely for OPIC business, and not for personal reasons.

(e) Computer-to-Analog Line Connections - The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within OPIC will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to the agency, and active penetrations have been launched against such lines by hackers. Waivers to the policy will be granted on a case-by-case basis.

(1) Requesting an Analog/ISDN Line - Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to IRM:

- A clearly detailed business case of why other secure connections available at OPIC cannot be used.
- The business purpose for which the analog line is to be used.

- The software and hardware to be connected to the line and used across the line.
- The sensitivity of the data to be transferred over the line.
- To what external connections the requester is seeking access.
- Whether the machines that are using the analog lines will be physically disconnected from OPIC's internal network.
- A description of where the analog line will be placed.
- Whether dial-in from outside of OPIC will be needed.
- The number of lines being requested, and how many people will use the lines?

(2) The line must be terminated as soon as it is no longer in use.

(f) Any connectivity between the telephone system and OPICNET must be approved by the OPIC Telecommunications Officer, the Director of Technical Services, and the ISSO.

(g) OPIC will adhere to NIST guidance as set forth in Special Publication 800-24, PBX Vulnerability Analysis, and other publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for deploying, managing, and protecting their telephony resources in compliance with OPIC information security policy.

(b) Information Custodians are responsible for assisting information owners with deploying, managing, and protecting their telephony resources in compliance with OPIC information security policy.

(c) The Information Systems Security Officer (ISSO) is responsible for auditing the use and management of OPIC telephony resources to ensure compliance with OPIC information security policies.

(d) Employees are responsible for using OPIC telephony resources in an ethical, responsible, and secure manner, in accordance with this policy and existing OPIC policies.

(e) Supervisors are responsible for ensuring that their employees understand and comply with this policy.

6. DEFINITIONS:

(a) Analog - A method of transmitting information in a continuous fashion via energy waves.

(b) ISDN - A type of communication line which can carry voice, digital network services and video.

(c) Modem - A device that enables a computer to transmit data over telephone lines by converting data between the computer's digital format and the phone line's analog format.

(d) Private Branch Exchange (PBX) - A private telephone switchboard that provides on-premises dial service and may provide connections to public communications networks.

(e) Sensitive Data/Information – Any data that is categorized as "sensitive" under OPIC's information resource classification policy and framework.

(f) Telephony - The technology associated with the electronic transmission of voice, fax, or other information between distant parties using systems historically associated with the telephone.

7. **ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

8. **POINT OF CONTACT:** OPIC Information Systems Security Officer (ISSO)

9. **ATTACHMENTS:** None

10. **AUTHORITY:**

(a) OPIC Directive 00-01, Information Systems Security Program.

(b) OPIC Directive 94-04, Personal Property Program Including Information Technology and Telecommunications.

(c) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.

(d) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

(e) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974.

11. **LOCATION:** TBD

12. **EFFECTIVE DATE:** October 22, 2004

13. **REVISION HISTORY:** None

14. **REVIEW SCHEDULE:** This policy should be reviewed and updated annually.