WIRELESS SECURITY

ISSP-27-0410

1. **SUBJECT:** When using wireless networks or handheld devices, OPIC should use its risk management processes to assess the risks involved with that particular technology, to take steps to reduce those risks to an acceptable level, and to ensure that a satisfactory level of protection is maintained.

2. **SCOPE:** This policy covers all wireless data communication devices connected to OPIC networks or which are used to transmit or store OPIC data.

3. **DESCRIPTION:** Many OPIC users have found that wireless communications and devices are convenient, flexible, and easy to use. From using a handheld device to send email to using wireless connectivity in their homes, users can benefit from the increased flexibility and availability of wireless access. There may also be potential opportunities to utilize wireless LAN and WAN connectivity in the OPIC office environment.

   In addition to the risks that apply to all networks, wireless connectivity is exposed to additional vulnerabilities. Wireless networks transmit data through radio frequencies, and their transmissions may be intercepted by anyone nearby who may be listening. Unless protected, all data transmitted through a wireless connection is open to the public. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tie up network bandwidth and deny service to authorized users. Additionally, portable wireless devices themselves are vulnerable to loss and theft, which could lead to exposure of stored data or unauthorized access to OPIC networks via the hijacked device.

   Because of the additional risks that are faced by wireless networks and devices, additional measures need to be taken to safeguard wireless connectivity and the data that is transmitted through it.

4. **PROCEDURES & GUIDELINES:**

   (a) The use of any wireless connectivity or device for accessing or transmitting OPIC information must be approved by IRM, regardless of whether these devices are owned by OPIC.

   (b) All OPIC wireless devices must be labeled and inventoried.

   (c) Users must report any lost or stolen wireless or handheld devices to their supervisor or the OPIC ISSO as soon as possible.

   (d) Access to OPIC and other systems and networks must be immediately terminated for any lost or stolen devices.

   (e) Access to any OPIC systems or networks using wireless devices or wireless networks must be authenticated.

   (f) Security risks and controls should be evaluated more frequently for wireless technologies than for other networks and systems.

(g) Periodic security testing and assessment should be performed for any OPIC wireless networks.

(h) Ongoing, randomly timed security audits should be used to monitor and track wireless and handheld devices.

(i) Patches and security enhancements should be applied to wireless networks in accordance with OPIC system security policy.

(j) Robust cryptography must be used whenever sensitive data is stored or transmitted on a wireless device.

(k) The SSID for each device should be configured such that it does not reveal any identifying information about OPIC.

(l) Inherent security features such as authentication and encryption methods that are available in wireless technologies should be tested and used.

(m) OPIC will adhere to NIST guidance as set forth in Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Users are responsible for:

(1) Adhering to OPIC procedures and guidelines regarding the use of wireless technologies, both within OPIC and when connecting to OPIC from remote locations.

(2) Safeguarding wireless devices in their possession.

(3) Safeguarding OPIC information resources being accessed or transmitted via any wireless technology.

(4) Promptly reporting the loss or theft of wireless devices, or any other breach of wireless security, to their supervisor or IRM.

(b) Supervisors are responsible for:

(1) Ensuring their employees understand and adhere to this policy.

(2) Forwarding reports of loss or theft of wireless devices to IRM.

(c) System Owners are responsible for:

(1) Using OPIC risk management procedures to ensure that risks have been analyzed and appropriately mitigated prior to, and during, use of any wireless technology resources that they own.

(2) Obtaining security approval prior to deploying any wireless technologies.

(3) Communicating wireless security policies and procedures to the users of their resources.

(d) System Custodians are responsible for:

(1) Safeguarding wireless information resources with which they have been entrusted.

(2) Adhering to OPIC policies and procedures for the administration of wireless devices, including:

- Labeling all wireless devices prior to deployment.
- Maintaining an inventory of all wireless devices.
- Disabling access or service for wireless devices that have been lost or stolen.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing the use of wireless technologies at, or in connection to, OPIC to ensure that appropriate security controls are used to mitigate risk.

6. DEFINITIONS:

(a) Authentication – The process of verifying that a user is who he or she purports to be. Techniques are usually broken down into three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or iris.

(b) Cryptography – A coding method in which data is encrypted (translated into an unreadable format) and then decrypted (translated back into a readable format by someone with a secret key) using an algorithm. Cryptography is used to send or store information securely.

(c) Encryption - The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy. Data is encoded to prevent unauthorized access.

(d) SSID – Short for **s**ervice **s**et **id**entifier, a unique identifier that acts as a password on a wireless network

(e) Wireless Technology – Any type of connectivity that transmits data without the use of physical cabling. Wireless systems include radio transmissions, satellite links, cell phones, and devices such as wireless headphones. Infrared (IR) devices such as remote controls, cordless computer keyboards, and cordless mouse devices are also included.

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

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

(d) NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices.

(e) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

11. LOCATION: TBD

12. EFFECTIVE DATE: October 22, 2004

13. REVISION HISTORY: None

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