REMOTE ACCESS

ISSP-25-0410

1. **SUBJECT:** Remote access requires additional security controls to mitigate the increased risks posed by allowing connectivity from outside the OPIC office environment.
2. **SCOPE:** This policy applies to all remote connectivity to OPIC information resources.
3. **DESCRIPTION:** Remote access to OPICNET provides many benefits. It allows personnel traveling on business to connect to OPIC information resources and provides the capability for telecommuting. However, remote access to OPIC via dial-up or other connectivity poses a risk of intrusion into OPICNET by unauthorized persons, as well as interception of the data being transferred through the remote connection. Direct connectivity to the Internet or other network outside of OPICNET also lacks the protections afforded by OPIC's corporate firewall and other perimeter protections. Additional security measures must be implemented to mitigate the increased security risks presented by remote access.
4. **PROCEDURES & GUIDELINES:**

   (a) All remote connectivity must be authenticated using strong or multi-factor authentication (such as the use of passwords in conjunction with tokens).

   (b) All sensitive data transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.

   (c) All security policies for use in the OPIC office environment must also be observed when using or connecting to OPIC resources while outside the OPIC office environment.

   (d) Any personal equipment, including personal home computers, used to connect to OPIC's information resources must meet OPIC remote access requirements, including having an approved antivirus program installed and configured with the latest updates.

   (e) OPIC sensitive data is not to be stored on any non-OPIC computers.

   (f) It is the responsibility of employees to ensure that their access devices and remote connections are not used by unauthorized persons (including family members).

   (g) Information users may not change operating system configurations, install new software, alter equipment or add to it in any way (*e.g.*, upgraded processors, expanded memory, or wireless cards), or download software from systems outside of OPIC onto OPIC remote access computers.

   (h) To prevent unauthorized users from accessing sensitive OPIC information via open modem ports, OPIC information users must log out rather than hang up after completing a remote session. They must also wait until they receive a

confirmation of their log-out command from the remotely connected OPIC machine before they leave the computer they are using.

(i) OPIC will adhere to NIST guidance as set forth in Special Publication 800-46, Security for Telecommuting and Broadband Communications, and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that any remote access to their information resources is conducted in accordance with the procedures and guidelines set forth in this policy.

(b) Information Custodians are responsible for assisting information owners with implementing the guidelines outlined in this policy.

(c) Information Users are responsible for:

(1) Complying with the procedures and guidelines set forth in this policy.

(2) Protecting their remote access credentials and devices from disclosure to, or use by, unauthorized persons.

(3) Immediately reporting any suspected unauthorized use of their remote access account or any damage to or loss of OPIC computer hardware, software, or data that has been entrusted to their care.

(d) Supervisors are responsible for ensuring that their employees understand and comply with these policies and guidelines.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing the use of remote access to ensure compliance with the procedures and guidelines set forth in this policy.

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) 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.

(c) Remote Access – Any access to OPIC's corporate network through a network, device, or medium that is not controlled by OPIC (such as the Internet, public phone line, wireless carrier, or other external connectivity).

(d) Sensitive Data – Any data that is categorized as “sensitive” under OPIC’s information resource classification policy and framework.

(e) Strong Authentication - An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by

eavesdropping. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.

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 03-01, Telecommuting Program

(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

(f) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(g) OMB Memo M-99-20, Security of Federal Automated Information Resources, June 1999.

(h) NIST Special Publication 800-46, Security for Telecommuting and Broadband Communications

(i) 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.