SECURITY TRAINING AND AWARENESS

ISSP-04-0410

1. **SUBJECT:** OPIC's information security policies and procedures will be communicated to all employees. They will be made available for reference and review by employees and any other persons who are in positions that can impact the security and integrity of OPIC information resources. A program to maintain effective awareness of information security policy, standards and acceptable practices will also be implemented. Additionally, persons responsible for administering or securing information resources must have adequate training on the proper implementation of security controls for the systems and data under their control.

2. **SCOPE:** This policy applies to all OPIC employees and contractors, including interns and temporary workers, who have access to OPIC information resources. The term "employees" will be used in this policy to specify all personnel within this scope.

3. **DESCRIPTION:** The Federal Information Security Management Act (FISMA) requires each federal agency to provide mandatory periodic information security training to all employees involved in the use or management of federal computer systems. Further, the Office of Management and Budget (OMB) Circular A-130 requires that such training be completed prior to the granting of access, and be provided for periodic refreshment.

   Aside from compliance with legal requirements, a Security Training and Awareness program is crucial to the safeguarding of OPIC information resources. Information security policy and standards cannot be effective unless everyone at OPIC, regardless of position in the organization, is aware of the importance of security, understands OPIC security procedures, and performs required practices. To make information security effective, standards and procedures must be known, understood, believed to be beneficial, and be appropriately and consistently practiced.

   Information Security is not a one-time event, but a continuous effort and "state of mind". This is achieved by reinforcing concerns and appropriate behaviors on a continuous basis. Effective information security is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments.

4. **PROCEDURES & GUIDELINES:**

   (a) OPIC will develop and maintain an Information Security Training and Awareness Program to educate employees about information security policies and procedures, and make them aware of their roles and responsibilities in safeguarding OPIC's information resources. The program will be composed of two major initiatives:

      (1) A Training program designed to build relevant and needed security skills and competencies to facilitate job performance.

(b) An Awareness program designed to focus attention on security, and to change behavior or reinforce good security practices. Ongoing development of security awareness builds a culture that encourages good security practices.

(c) All information users will complete training on OPIC Information security policies and procedures. This will consist of three (3) training activities:

(1) Information security training will be incorporated into the orientation processes for all new staff. Training must be completed within 30 days of employment or initiation of contract.

(2) All information users will complete an annual Information security training program to refresh their knowledge of information security.

(3) Information Custodians and other personnel with responsibilities related to administering and securing systems will be provided with enhanced security training applicable to their functions.

(d) OPIC will maintain and publish an Information Security Handbook documenting policies, procedures, and responsibilities.

(e) On an annual basis, employees will sign an agreement that they understand the OPIC Information security policies and procedures and that they will abide by them.

(f) Employees will be made aware of the penalties for non-compliance with OPIC security policies and procedures.

(g) Materials will be posted or presented in a variety of formats on a regular basis to maintain user awareness of information security issues.

(h) Changes to OPIC Information security policies or procedures will be communicated to all information users.

(i) OPIC will adhere to NIST guidance as set forth in NIST Special Publication 800-50, Building an Information Technology Security Training and Awareness Program, and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

(a) The Information Systems Security Officer (ISSO) is responsible for developing and operating the Information Security Training & Awareness program, including:

(1) preparing policy on security awareness and training,

(2) developing and presenting security training courses and briefings,

(3) developing and distributing awareness material and bulletins, and ensuring all personnel receive the appropriate security training associated with their jobs, and

(4) maintaining records of training received.

(b) Supervisors and COTRs are responsible for:

(1) Ensuring that their employees are briefed and understand their roles in implementing OPIC's Information Security program.

(2) Communicating changes in policies and procedures to their staff.

(3) Providing opportunities for staff to complete information security training.

(4) Assisting with the monitoring of information security compliance within their departments.

(c) Information Users are responsible for:

(1) Completing annual security training.

(2) Reviewing and understanding OPIC information security policies and procedures.

(3) Completing and abiding by the "Agreement To Comply With OPIC Information Security Policy" document.

(4) Complying with all OPIC information security policies and procedures.

(d) Information Owners are responsible for ensuring that personnel who use their resources are appropriately trained to fulfill their security responsibilities for those resources.

6. **DEFINITIONS:**

(a) Awareness – A state of focused attention on security that allows individuals to recognize IT security concerns and respond accordingly.

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:

(a) Agreement To Comply With OPIC Information Security Policy

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) Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.

(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) Computer Security Act of 1987, PL 100-235, January 8, 1988.

(g) NIST Special Publication 800-50, Building an Information Technology Security Training and Awareness Program.

(h) 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.