SYSTEM SECURITY PLANS

ISSP-07-0410

1. **SUBJECT:** Each major information system must have an approved security plan.
2. **SCOPE:** This policy covers all major OPIC information systems.
3. **DESCRIPTION:** A security plan lists security requirements, defines risks, and describes security measures to be implemented for a particular system. This helps to ensure that a security risk analysis is performed for the system, and that appropriate security controls are put in place. The security plan also defines roles and responsibilities for security of the system, as well as standard operating procedures.
4. **PROCEDURES & GUIDELINES:**

   (a) Each new major information system must have an approved Security Plan before going into operation.

   (b) Owners of existing major information systems that do not have an approved Security Plan must develop one as soon as possible.

   (c) Each System Security Plan must be reviewed, updated, and re-approved at least once every two years, or when there is a major change to the system, whichever is earlier.

   (d) The System Security Plan will be used as a critical component of the Certification and Accreditation of the system.

   (e) Other organizations or systems that are connected to or share data with the OPIC system must have a Memorandum of Understanding (MOU) or other formal documented agreement that describes the rules governing the interconnection.

   (f) System Security Plans must be marked, handled, and controlled as sensitive but unclassified information.

   (g) OPIC will adhere to NIST guidance as set forth in Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

   (a) Information Owners are responsible for:

   (1) Ensuring that System Security Plans are developed for the systems that they own.

   (2) Formally approving and accepting system security plans for their systems.

   (b) Information Custodians are responsible for assisting Information Owners and the ISSO with the development and implementation of System Security Plans.

   (c) The Information Systems Security Officer (ISSO) is responsible for:

   (1) Assisting with the development and review of system security plans.

(2) Auditing systems to ensure that their security plans have been effectively implemented.

6. DEFINITIONS:

(a) Major Information System – An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

(b) Memorandum of Understanding (MOU) - A document providing a general description of the responsibilities that are to be assumed by two or more parties in their pursuit of some goal(s).

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) 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) OMB Circular A-123, Internal Control Systems, August 4, 1986.

(f) NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems.

(g) 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.