RISK MANAGEMENT

ISSP-03-0410

1. **SUBJECT:** OPIC must develop, implement, and maintain a risk management program to ensure that appropriate safeguards are employed to protect OPIC resources.
2. **SCOPE:** This policy applies to all OPIC information resources.
3. **DESCRIPTION:** In determining a security strategy for a system or the organization, OPIC must determine the correct balance between mitigating risks and expending resources. Appropriate controls must be implemented to protect against the occurrence of serious threats to the business, while addressing financial and operational concerns. The objective of performing risk management is to enable OPIC to accomplish its mission by:

   - ❖ Better securing the IT systems that store, process, or transmit organizational information.
   - ❖ Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget.
   - ❖ Assisting management in authorizing (or accrediting) their IT systems on the basis of the supporting documentation resulting from the performance of risk management.

   Risk management is an essential management function and should not be treated solely as a technical function relegated to IT operational or security personnel for implementation. Effective risk management processes support sound *risk-based decision-making*. The CIO and other OPIC executives need to ensure implementation of an effective and comprehensive risk management program, which encompasses all segments of the enterprise, in order to support OPIC's mission.

4. **PROCEDURES & GUIDELINES:**

   (a) OPIC will use a risk-based approach to determine information security requirements to ensure that security is commensurate with the risk and magnitude of harm that can result from the loss, misuse, unauthorized access to, or modification of, OPIC information.

   (b) OPIC management will make all information technology decisions based on a thorough analysis of the risks involved.

   (c) Risk management procedures must be integrated into OPIC's systems development life cycle (SDLC). Risk management is an iterative process and has activities relevant to every phase of the life cycle. Security considerations must be included in the initiation, development/acquisition, implementation, operation/maintenance, and disposal of all OPIC information resources.

   (d) Risk management is a cyclical process and must be performed on an ongoing basis for all information resources.

(e) OPIC will adhere to NIST guidance as set forth in Special Publication 800-30, Risk Management and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners and OPIC Executives are responsible for:

(1) Committing to performing on-going periodic risk management of information resources.

(2) Considering the results of a risk assessment in making decisions about the use of information resources.

(3) Implementing appropriate safeguards based on the results of risk analysis.

(b) Information Custodians are responsible for:

(1) Assisting with the assessment and mitigation of risks for the information resources with which they have been entrusted.

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

(1) Developing OPIC risk management procedures.

(2) Conducting risk assessments on OPIC information systems.

(3) Identifying potential threats to the confidentiality, integrity, and availability of OPIC information resources.

(4) Performing vulnerability testing in accordance with OPIC policies and procedures.

(5) Providing recommendations for the cost-effective mitigation of risks to information resources.

6. DEFINITIONS:

(a) Availability - Assuring information and communications services will be ready for use when expected

(b) Confidentiality - Assuring information will be kept secret, with access limited to appropriate persons.

(c) Integrity - Assuring information will not be accidentally or maliciously altered or destroyed. Information has integrity when it is timely, accurate, complete, and consistent.

(d) Risk – The possibility of something adversely affecting the confidentiality, availability and integrity of OPIC's information resources.

(e) Risk Assessment - The process of analyzing and interpreting risk. Risk assessment is used to identify security risks, examine threats to and vulnerabilities of systems, determine the magnitude of risks, identify areas needing safeguarding, and determine the acceptability of risk.

(f) Risk Management – The process of identifying risk, assessing riskRisk, and taking steps to reduce risk to an acceptable level. The risk management process allows OPIC to balance the operational and economic costs of protective measures and

achieve gains in mission capability by protecting the IT systems and data that support the agency's mission.

(g) Threat - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

(h) Vulnerability – Any characteristic of a computer system that renders it susceptible to destruction or incapacitation. A design, administrative, or implementation weakness or flaw in hardware, firmware, or software that, if exploited (either intentionally or accidentally), could lead to an unacceptable impact in the form of unauthorized access to information or disruption of critical processing.

(i) Vulnerability Testing – Systematic examination of a system to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

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

(e) NIST Special Publication 800-30, Risk Management.

(f) 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.