INFORMATION RESOURCE CLASSIFICATION

ISSP-02-0410

1. **SUBJECT:** All information resources (including data and systems) must be identified, categorized, and protected according to their level of sensitivity, criticality, and business "need to know."

2. **SCOPE:** This policy applies to all OPIC information systems and data created, owned, stored, or transferred by OPIC that are not designated as national security classified.

3. **DESCRIPTION:** In order to ensure that appropriate levels of protection are applied to information resources, a framework is needed to classify those resources based on their criticality to the organization and the sensitivity of the data that they contain. This includes developing procedures and standards for assessing the criticality and sensitivity of the systems, and determining minimum security requirements based on those classification levels.

4. **PROCEDURES & GUIDELINES:**

   (a) All OPIC information resources will be categorized based on OPIC's information classification framework.

   (b) Risks and threats to information resources will be assessed, and security measures will be applied, based on the resource's classification level, in accordance with OPIC risk management procedures.

   (c) OPIC's information classification framework will be based on NIST guidance, as presented in FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, and Special Publication 800-60, Guide For Mapping Types of Information and Information Systems to Security Categories, as well as subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

   (a) Information Owners are responsible for:

      (1) Categorizing their resources in accordance with OPIC's classification framework.

      (2) Ensuring that their resources are protected commensurate with their categorization level.

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

      (1) Developing and communicating OPIC's information classification framework.

      (2) Assisting information owners with assessing the classification level of their resources.

      (3) Auditing to ensure compliance with this policy.

6. **DEFINITIONS:**

(a) Information Resources – The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

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

(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) Presidential Decision Directive 67, Continuity of Operations, October 21, 1998.

(h) FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems

(i) NIST Special Publication 800-60, Guide For Mapping Types of Information and Information Systems to Security Categories.

(j) 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.