ASSET MANAGEMENT

ISSP-33-0410

1. **SUBJECT:** All information assets must be tracked and managed to ensure that they are not lost or misused.

2. **SCOPE:** This policy applies to all OPIC information assets, including but not limited to workstations, servers, network devices, printers, personal digital assistants (PDAs), phones, software, and licenses.

3. **DESCRIPTION:** Each year, thousands of information assets are lost or stolen. Often agencies simply lose track of these items, sometimes resulting in scandals that appear in the news, and at minimum incurring the wrath of auditing organizations like GAO and OMB.

   Not only would loss of information assets result in a financial impact on OPIC, but it could also result in unauthorized access to data stored on or accessed through these assets, and could have a detrimental effect on the reputation of the agency. Additionally, the tracking and management of information assets is mandated by several federal regulations, such as the Clinger-Cohen Act.

4. **PROCEDURES & GUIDELINES:**

   (a) OPIC must keep a record of all information assets, including those mentioned in the scope above.

   (1) Information assets are to be added to the record upon receipt by OPIC and assigned a barcode.

   (2) For each information asset, OPIC will track at least the following information:

   - The brand, model, and type of asset
   - Serial number and OPIC barcode
   - The person to whom the asset is assigned
   - The location of the asset
   - Any maintenance agreements for the asset
   - The date of receipt of the item
   - Date the record was last updated or inventoried

   (3) Upon disposal of an information asset, OPIC will track the date of disposal, the method of disposal (e.g., transfer, destruction, donation, etc.), and the name of the new owner (if there is one).

   (b) Periodic inventories are to be performed to verify records and account for all information assets.

   (1) Each asset is to be inventoried at least annually.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for inventorying, tracking, and protecting the OPIC information resources that they own.

(b) Information Custodians are responsible for assisting information owners with inventorying, tracking, and protecting OPIC information resources in their care.

(c) Information Users are responsible for exercising due diligence in protecting information resources entrusted to them, and immediately reporting the loss, theft or damage of any OPIC information resource.

(d) Supervisors are responsible for ensuring their employees understand their responsibilities regarding protection of information resources.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing to ensure that information assets are being tracked and managed in accordance with this policy.

6. DEFINITIONS:

(a) Information Asset – An information resource that has tangible value.

(b) Information Resource - 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) Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.

(e) Federal Managers Financial Integrity Act of 1982 PL 97-255 (H.R. 1526).

11. LOCATION: TBD

12. EFFECTIVE DATE: October 22, 2004

13. REVISION HISTORY: None

14. REVIEW SCHEDULE: This policy should be reviewed and updated annually.