AUDIT TRAILS

ISSP-13-0410

1. **SUBJECT:** Audit trails must be maintained to provide accountability for the use of OPIC's information resources.
2. **SCOPE:** This policy applies to all OPIC information systems and all information users.
3. **DESCRIPTION:** In order to enforce information usage policies and security measures, and to be able to investigate security incidents, automated logs of access to and alteration of information systems and data must be maintained. To accomplish this, a record of activity (or "audit trail") of system and application processes and user activity of systems and applications must be maintained. This is used to investigate security incidents, monitor use of OPIC resources, provide accountability for transactions, track system changes, and assist in detection of system anomalies. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.
4. **PROCEDURES & GUIDELINES:**

   (a) Audit Trails will be maintained for OPIC information systems:

   (1) At minimum, the following transactions should be logged for each server:

   - Server startup and shutdown
   - Loading and unloading of services
   - Installation and removal of software
   - System alerts and error messages
   - User logon and logoff
   - System administration activities
   - Accesses to sensitive information and systems
   - Modifications of privileges and access controls
   - Additional security related events

   (2) At minimum, the following transactions should be logged for each application:

   - Modifications to the application
   - Application alerts and error messages
   - User sign on and sign off
   - System administration activities

- Accesses to sensitive information
- Modifications of privileges and access controls

(3) At minimum, the following transactions should be logged for each router, firewall, or other major network device:

- Device startup and shutdown
- Administrator logon and logoff
- Configuration changes
- Account creation, modification, or deletion
- Modifications of privileges and access controls
- System alerts and error messages

(4) Type of event, date, time, and user identification must be recorded for each logged transaction.

(5) Sensitive information, such as passwords and actual system data, should not be stored in the logs.

(b) Periodic reviews of audit logs will be conducted by the ISSO or other designated personnel.

(c) Only designated personnel should have access to the audit logs.

(d) Audit trail files are to be kept for at least one (1) year.

(1) Audit trails associated with known incidents (including those used for legal action) are to be kept for three (3) years.

(e) Audit trails must be kept in a secure location. Audit data should be some of the most carefully secured data at the site and in the backups. If an intruder were to gain access to audit logs, the systems themselves, in addition to the data, would be at risk.

(f) OPIC will follow NIST guidance regarding audit trails.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that audit trails are implemented and maintained for their resources.

(b) Information Custodians are responsible for assisting information owners with implementing and maintaining audit trails for the resources for which they are responsible.

(c) Supervisors are responsible for assisting the ISSO in reconciling audit trail anomalies.

(d) The Information Systems Security Officer (ISSO) is responsible for periodically reviewing audit trails for all systems to ensure compliance with this policy.

(e) Information Users are responsible for understanding and acknowledging that their use of OPIC systems may be logged and audited.

6. DEFINITIONS:

(a) Audit Trail - In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

(b) Security Incident - Any activity that is a threat to the availability, integrity, or confidentiality of information resources, or any action that is in violation of security policies

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) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

(e) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

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

(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.