CHANGE CONTROL

ISSP-18-0410

1. **SUBJECT:** Authorized changes must occur to OPIC's network and information systems, and these changes must occur in a timely manner without disruption or compromise to existing system operation. However, OPIC must protect its information systems from unauthorized changes, intrusions or misuse. One way of facilitating this requirement is to formally manage and control hardware and software configuration changes.

2. **SCOPE:** This policy applies to all OPIC information systems.

3. **DESCRIPTION:** Change control involves controlling and managing changes to OPIC's information systems to ensure integrity of data and information. OPIC information systems require appropriate administrative, physical and technical controls to be incorporated into both new additions and changes to systems. These controls must encompass not only the software, but also the routine activities that enable OPIC's information systems to function properly (*e.g.*, fixing software or hardware problems, loading and maintaining software, updating hardware and software, and maintaining a historical record of application changes). Change control prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems.

   Informal operational processes with no means of controlling changes to information systems impede OPIC's ability to determine the status of its current architecture, network component configuration and even to propose changes. Change control planning addresses this deficiency and establishes a consistent, cross-organizational change management process for OPIC information systems. Change control history lays the framework of how OPIC's network is built and is a valuable tool for both emergency response and information architecture planning.

4. **PROCEDURES & GUIDELINES:**

   (a) Changes to each OPIC information system will be systematically planned, approved, tested and documented at a level appropriate with the size, complexity, and sensitivity of the system.

   (b) OPIC will develop baseline information that includes a current list of all components (hardware, software, and their documentatio n), configuration of peripherals, version releases of current software, information on batch files, environmental settings such as paths, and switch settings of machine components.

   (c) For each information system, OPIC will maintain a log of all configuration changes made, the name of the person who performed the change, the date of the change, the purpose of the change, and any observations made during the course of the change.

(d) Procedures will be implemented to ensure that maintenance and repair activities are accomplished without adversely affecting system security. The procedures shall:

(1) Establish who performs maintenance and repair activities.

(2) Contain procedures for performance of emergency repair and maintenance.

(3) Contain the management of hardware/software warranties and upgrade policies to maximize use of such items to minimize costs.

(e) Version control that associates system components to the appropriate system version will be followed.

(f) Impact analyses will be conducted to determine the effect of proposed changes on existing systems and security controls.

(g) Procedures will be implemented for testing and/or approving system components (operating system, other system, utility, applications) and configuration changes prior to promotion to production.

(h) Information Users will be notified regarding how they will be impacted by changes.

(i) Current backups will be available when changes are made.

(j) All software, operating systems, and patches shall be installed in accordance with U.S. copyright regulations, the license for that software, and applicable OPIC Information Security policies.

(k) Only authorized personnel may make changes to OPIC information systems.

(l) Change control procedures will be documented for all systems to provide a complete audit trail of decisions and design modifications.

(m) Change control documentation (especially change logs) will be available even if the network is down and will not contain passwords for affected components.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for ensuring that changes to the systems they own are documented and implemented in compliance with the policies and procedures listed in this document.

(b) Information Custodians are responsible for:

(1) participating in the development of procedures for change control.

(2) evaluating, recommending, and coordinating the implementation of solutions/changes consistent with OPIC technical plans.

(3) maintaining change log documentation.

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

(1) developing change control procedures.

(2) working with Information Owners and Custodians to ensure that change control policies and procedures are followed and documented.

(3) monitoring OPIC information systems to ensure compliance with this policy.

6. DEFINITIONS:

(a) Change Control - Documented procedures used to control the revision of applications, operating systems, and hardware configurations in computing environments.

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) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

(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.