PATCH MANAGEMENT AND SYSTEM UPDATES

ISSP-20-0410

1. **SUBJECT:** OPIC information systems are to be maintained with updated security patches.
2. **SCOPE:** This policy covers all servers, operating systems (OS), workstations, network devices, applications, and other information resources for which vendors provide system patches or security updates.
3. **DESCRIPTION:** Maintained patch levels are critical to the security of OPIC systems. Vendors will typically provide OS patches and fixes for security problems, which can be loaded separately from the application. These should be loaded on a regular basis using a coordinated process.
4. **PROCEDURES & GUIDELINES:**
   a) A patch management program that includes detailed procedures and standards will be developed and implemented across OPIC information resources.
   b) During regular operation, available patches will be reviewed monthly and applied if appropriate. In an emergency situation (such as an ongoing security incident), more urgent application of new security patches may be required.
   c) Patches will be checked for compatibility with all system components prior to being applied.
   d) Patches will be successfully tested on non-production systems prior to being loaded on production systems.
   e) Patching should be performed during an authorized outage window unless there is an urgent situation.
   f) Systems will be backed up prior to installation of new patches.
   g) All systems that are a part of the network infrastructure will have a log book. System log books help record the status of network equipment and provide continuity among administrators. The log book may be in paper or electronic form. Information to be recorded includes: date of the action, administrator's name, patches and patch numbers that were installed, problems encountered, and system administrator remarks.
   h) In the event that a system must be reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the patch levels in effect before reloading.
   i) OPIC will adhere to NIST guidance as set forth in Special Publication 800-40, Procedures for Handling Security Patches, and subsequent publications.
5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that their information resources are maintained in compliance with OPIC patch management policies and procedures.

(b) Information Custodians are responsible for assisting information owners with the development and implementation of patch management policies and procedures for their information resources.

(c) The Information Systems Security Officer (ISSO) is responsible for auditing information systems to ensure that they comply with OPIC patch management policies and procedures.

6. **DEFINITIONS:**

(a) Network Device – Any physical component which forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc.

(b) Network Infrastructure – Network infrastructure includes servers, network devices, and any other back-office equipment.

(c) Patch – A patch is a 'fix' to a known problem with a piece of software. Instead of redistributing the entire new version of a program a patch, which is much smaller, can be applied to the old version.

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) NIST Special Publication 800-40, Procedures for Handling Security Patches

(e) 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.