# NETWORK SECURITY

ISSP-23-0410

1. **SUBJECT:** Network devices and connectivity components should be made secure before placing them into the OPIC operational information technology environment, and security should be maintained throughout their lifecycle.
2. **SCOPE:** This policy applies to all routers, switches, cabling, and other network components that are part of OPIC's connectivity infrastructure.
3. **DESCRIPTION:** It takes only one incorrectly configured system to allow an intruder into OPIC's network. No network components should ever be implemented without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements made available, the configuration of the network must continually be updated to maintain security vigilance.
4. **PROCEDURES & GUIDELINES:**

   (a) Standard base security configurations will be developed for each type of network component (*i.e.* routers, switches, etc.) and applied to all such components.

   (b) The level of security applied to each network component should be commensurate with the level of criticality and sensitivity of the data transmitted over, and services provided by, that network.

   (c) Patch Management:

      (1) Patches and security updates must be applied in a timely fashion in accordance with OPIC patch management procedures.

      (2) Logs must be kept documenting the patches and updates that have been installed on each device, including at minimum the name of the device, the name of the patch, the version of the patch, the date of installation, and the name of the person who installed the patch.

   (d) Any unnecessary services will be disabled. (For example, if a router does not need to be managed by SNMP, then SNMP should be disabled).

   (e) Access to all OPIC network devices must adhere to the OPIC Access Control and Identification and Authentication policies.

   (f) Remote administration of network devices can only be performed using encrypted and authenticated connections.

   (g) Auditing and logging must be enabled in accordance with OPIC auditing policies and procedures.

   (h) Warning banners that specify access requirements and penalties for unauthorized access will be provided upon access to the network or device.

   (i) Each device must be inventoried and tracked in accordance with OPIC asset management policies and procedures.

(j) Each device's configuration must be thoroughly documented, and this documentation must be kept up to date.

(k) Any changes made to the configuration of a device must be performed in accordance with OPIC change management policies and procedures.

(l) Network devices will be located in access-controlled and environmentally-protected facilities, in accordance with OPIC physical and environmental security policies and procedures.

(m) No device may be connected to the OPIC network without approval from the Director of Technical Services.

(n) No non-OPIC computers (e.g., contractor-owned or personal laptops) may be directly connected to the OPIC network.

(o) All network components must be assigned an owner and a custodian.

(1) These roles can be assigned to the same person or different people.

(2) Owners must be OPIC personnel. Custodians can be employees or contractors.

(p) OPIC will adhere to NIST and NSA hardening guidance for routers and other networking components, as appropriate.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that any network components they own are in compliance with the guidelines provided by this policy.

(b) Information Custodians are responsible for assisting information owners with implementing the guidelines provided by this policy.

(c) The Information Systems Security Officer (ISSO) is responsible for auditing network components to ensure that they are configured in accordance with the guidelines provided by this policy.

6. **DEFINITIONS:**

(a) Hardening – The process of disabling unnecessary services, installing all the latest patches, installing security software (*e.g.*, anti-virus software), tuning the operating system, and documenting the system.

(b) 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.

(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.

(d) Router – A device that interconnects networks and directs and filters traffic between them.

(e) Switch – A physical component that connects multiple computers and devices to a network.

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

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

    (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.