SERVER SECURITY

ISSP-21-0410

1. **SUBJECT:** Servers 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 OPIC information servers, including file and print servers, application servers, and database servers. All operating systems associated with these servers are also included.
3. **DESCRIPTION:** It takes only one incorrectly configured system to allow an intruder into OPIC's network. No server should ever be placed on the network without a proper security configuration.

   Additionally, as new vulnerabilities are discovered and additional security enhancements are made available, the security of the servers must continually be updated to maintain security vigilance.

4. **PROCEDURES & GUIDELINES:**

   (a) Standard base security configurations will be developed for each type of server and applied to all servers.

   (b) The level of security applied to each server will be commensurate with the level of criticality and sensitivity of the data and services that it provides.

   (c) Patch Management:

      (1) System 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 server, including at minimum the name of the server, 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 (*e.g.*, if a mail server does not need to allow File Transfer Protocol (FTP), then FTP should be disabled).

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

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

   (g) All servers must run antivirus software configured in accordance with OPIC antivirus policies and procedures.

   (h) Warning banners that specify requirements and penalties for accessing the system will be provided upon access to the server.

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

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

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

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

(m) Procedures will be implemented to provide verifiable backups of all servers, in accordance with OPIC data backup policies and procedures.

(n) All servers must be assigned an Information 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.

(o) OPIC will adhere to NIST and NSA hardening guidance for servers, as appropriate.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for ensuring that any servers 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 servers 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) 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.

(c) Server – Computer that provides a service or application that users access through a network connection.

(d) Strong Authentication – An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by eavesdropping. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.

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.