5 FAM 860 HARDWARE AND SOFTWARE MAINTENANCE

(TL:IM-50; 05-04-2004)
(Office of Origin: IRM/APR/RG)

5 FAM 861 CONFIGURATION MANAGEMENT

(TL:IM-50; 05-04-2004)

a. Configuration management provides assurance that an information system in operation is the correct configuration and that any changes made are reviewed for security ramifications. Configuration management ensures that changes take place in an identifiable and controlled fashion and cannot adversely affect any of the information system's functionality, including its security posture.

b. The Information Management Officer (IMO)/Information Systems Officer (ISO)/System Administrator must configure both OpenNet and ClassNet information systems in accordance with the standards established by IRM/OPS/ENM and Department guidelines, developed by Diplomatic Security.

c. The IT CCB must approve each change to a network that affects more than a single domain (local network segment). Changes that affect only a single domain or Local Area Network (LAN) may be approved by a Local CCB. Guidance on establishing a Local CCB may be found at 5 FAM 862.

d. IMOs/ISOs/System Administrators must oversee and enforce configuration management principles on all systems, including hardware and software. To support this activity, IMOs/ISOs/System Administrators will develop and maintain a Configuration Management Plan for their domains.

5 FAM 862 LOCAL CHANGE CONTROL BOARDS

(TL:IM-50; 05-04-2004)

5 FAM 862.1 Responsibilities of a Local CCB

(TL:IM-50; 05-04-2004)

a. Each post and bureau that has systems or applications for which it is responsible must establish a Local CCB.

b. The purpose of the Local CCB is to ensure that any hardware, software, or network component installed on a LAN does not adversely affect the existing local IT infrastructure under the operational control of bureau/post IT personnel. The Local CCB must also ensure that all locally approved software and hardware functions inside the local network segment.

c. Each Local CCB is responsible for maintaining its contact with IT CCB Voting Representative.

5 FAM 862.2 Local CCB memberships

(TL:IM-50; 05-04-2004)

The Local CCB should consist of a Local CCB chairperson and added members as appropriate. For generic information, see ENM/IRM web site.

5 FAM 862.3 Determining what must be sent to the IT CCB

(TL:IM-50; 05-04-2004)

If the Local CCB determines that an application would function outside the local domain or LAN it must obtain IT CCB approval to use the application. See ENM/IRM web site for information on Local CCB and IT CCB.

5 FAM 863 OPERATING SYSTEM SOFTWARE

(TL:IM-50; 05-04-2004)

System Administrators must notify DS before installing operating systems software that has not been used before in the Department. See 12 FAM 623 and 12 FAM 633. For a list of currently approved operating system software, see the IT CCB web site.

5 FAM 864 APPLICATION SOFTWARE AND CHANGE CONTROL

(TL:IM-50; 05-04-2004)

a. Software change controls must be implemented for major and developed applications installed on Department systems.

b. Each System Owner must ensure implementation of the following application software controls for each information system:

(1) defining requirements, including security, in the system development and acquisition stage for system confidentiality and availability as well as integrity of data input, transaction processing, and data output;

(2) initiating the systems authorization process;

(3) testing the application in a development environment, or test bed, prior to operation to ensure the presence of satisfactory operation of controls (this is usually the certification process);

(4) monitoring security controls for vulnerabilities throughout the deployment, operation, and maintenance stages;

(5) limiting access to software programming libraries; and

(6) protecting system documentation with the same due diligence as the data are protected.

c. Each System Owner must ensure integrity of major applications and operating system software by implementing documented and effective configuration management procedures, including procedures to:

(1) restrict the ability to change software (update, upgrade, install, and uninstall) to only those authorized by the system owner;

(2) audit all changes and maintain a secure copy of the audit;

(3) maintain a secure copy of changes (old and new software); and

(4) test all changes on non-live data before deploying changes in a live environment.

d. Each application must be approved either by the Department IT CCB or by the local CCB, as appropriate, before it is used. See 5 FAM 862.3.

e. All custom built applications must be placed into Information Technology Application Baseline (ITAB), which must be updated whenever such applications are changed. Posts and bureaus are responsible for providing updates to the ITAB for applications they develop or purchase. See the ITAB web site for instructions on adding and updating information in the ITAB.

5 FAM 865 COPYRIGHTED SOFTWARE

(TL:IM-50; 05-04-2004)

Department employees and contractors may use and distribute commercial software only in accordance with U.S. copyright laws and manufacturing licensing agreements.

5 FAM 866 PATCH MANAGEMENT

(TL:IM-50; 05-04-2004)

a. The purpose of the Department's Enterprise Patch Management Program is to protect data confidentiality, integrity, and availability by mitigating software and hardware vulnerabilities through proactive patch management.

b. IRM/OPS/ENM/NLM manages the Department's Enterprise Patch Management Program.

c. IMOs/ISOs/System Administrators must follow guideline and procedures established by the Department's Enterprise Patch Management Program and apply patches in an expeditious manner.

d. The Designated Approval Authority (DAA) may disconnect any system, LAN, or domain that does not comply with the Department's Enterprise Patch Management Program's directives.

5 FAM 867 DOCUMENTATION

(TL:IM-50; 05-04-2004)

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Documentation must include:

(1) Current security plans, contingency plans, and risk analyses;

(2) Sufficient documentation to explain how software/hardware is used, including operational procedures;

(3) A current list of workstations (including stand-alones), printers, servers, and other network peripherals/devices (e.g., scanner), the office in which each is located, the cable number/ device number, and port in the hub/switch/router where each is located;

(4) A current list of all the software applications used, the names of the principal users, and the person/office to contact for operational issues or problems;

(5) An annual system performance report;

(6) A systems operations log. This log must be maintained for six months. See 12FAM 629.2-11 Log and Record Keeping or 12 FAM 632.5 Log and Record Keeping;

(7) An annual security self-assessment, in accordance with guidance IRM/IA will provide each year;

(8) Audit records on servers and workstations for six (6) consecutive months; and

(9) The current configuration management plan for the bureau/post.

5 FAM 868 THROUGH 869 UNASSIGNED