5 FAM 860  
HARDWARE AND SOFTWARE MAINTENANCE  
*(CT:IM-145; 07-12-2013)*  
*(Office of Origin: IRM/BMP/GRP/SM)*

5 FAM 861  CONFIGURATION MANAGEMENT

5 FAM 861.1  Overall Department Policy  
*(CT:IM-145; 07-12-2013)*

a. Configuration management (CM) is the detailed recording and updating of information that describes Department information systems and networks, including all hardware and software components. Configuration management records versions and updates applied to installed software packages and the locations and network addresses of hardware devices. When a system needs a hardware or software upgrade, a system manager can access the configuration management program and database to see what is currently installed. The system manager can then make a more informed decision about the upgrade needed.

b. Developers use configuration management in software development to help keep track of the source code, documentation, problems, and changes requested and implemented.

c. Configuration management provides assurance that an information system in the operational/maintenance phase of its lifecycle is the correct configuration and that any changes made are reviewed for security ramifications by the Information Technology Configuration Control Board (IT CCB) IA reviewer and the appropriate Bureau of Diplomatic Security reviewer for security implication and approval prior to implementation. Configuration management ensures that changes take place in an identifiable and controlled fashion and have been tested to preclude adverse effects on the information system’s functionality, including its security posture or any connecting Department information system’s security posture.

d. Configure Department information systems in accordance with the standards established by Information Technology Configuration Control Board (IT CCB) and the Bureau of Diplomatic Security (DS).

e. The IT CCB must approve any Network capacity changes, prior to implementation that may cause effects outside of the post and post's tail circuits. A local IT CCB may approve changes that affect only LANs or VLANs within the post and its tail circuits. For systems where system security plans
are no longer required, include all documentation recording any network changes approved by the local IT CCB in the affected system’s security documentation (i.e., systems security plan (SSP), contingency plan (CP), etc.). Local IT CCBs must process and record their changes through the Department’s change control application so that one central database stores all changes and approvals for applications and hardware.

f. For those systems which **do not** fall under the OpenNet or Classnet C&A, information management officers (IMOs), information security officers (ISOs), information system security officers (ISSOs), and system administrators must develop and maintain Department configuration management plans on all Department information systems and the networks under his or her management authority, as part of a system’s security documentation required to undergo certification and accreditation (C&A).

### 5 FAM 861.2 Standard Operating Environments

**CT:IM-145; 07-12-2013**

a. A Standard Operating Environment (SOE) is a specification for using a standard architecture and applications within a Department information system.

b. An SOE supports development of strong configuration management plans for the computing environments commonly used throughout the Department.

c. An SOE is a subset of the overall IT CCB-approved hardware and software baselines approved for Department use, for example, the SOE for desktops or servers.

d. Use of an SOE ensures that the following goals are met:

   (1) Efficiently and effectively maintain the components of an SOE. The Department authorizes only IT CCB-approved development, implementation, configuration, deployment, and upgrade methods. Regular voting by the IT CCB ensures that the SOE is regularly updated. Communication channels of the IT CCB (meetings, website, standard forms, etc.) ensure that current and future forms of the SOE are effectively communicated throughout the Department;

   (2) All components of an SOE are expected to have a standard life-cycle, which consists of implementation, maintenance, and ultimate disposal and removal from the IT CCB-approved baseline. Only current Department-supported or approved vendor versions of SOE components can exist within the Department;

   (3) There are a limited number of versions of any component on an SOE;

   (4) The IT CCB must approve new versions of components comprising an SOE. A local IT CCB does not have approval authority for approving new versions of SOE components;
(5) Ensure that all SOE components previously approved by the IT CCB are compatible with new SOE components. You must upgrade or remove previous IT CCB-approved hardware and software that is not compatible with new SOE components as directed by the IT CCB;

(6) The configuration of the SOE must comply with appropriate Department information security and configuration standards. (See 12 FAM 600 and the DS/SI/CS IT Security Configuration Standards website);

(7) Outline any exclusion to this policy in the IT CCB Standard Operating Procedure (SOP) available on the IT CCB website; and

(8) In accordance with 5 FAM 915.14, the IT CCB administers the creation, maintenance, and deactivation of components comprising an SOE. (See the IT CCB SOP.)

5 FAM 861.3 Minimum Hardware Specifications
(CT:IM-135; 10-10-2012)

a. Global IT Modernization Program (GITM) sets the minimum hardware baseline.

b. Updated annually, the specifications reflect the current, deployed systems both by the GITM program and by Desktop Support. The IT CCB website contains the current specifications. The oldest hardware that can be on the network must meet the GITM minimum hardware specifications.

5 FAM 862 LOCAL CONFIGURATION CONTROL BOARDS

5 FAM 862.1 Local IT CCB Responsibilities
(CT:IM-145; 07-12-2013)

a. A post or bureau that maintains its own IT systems or in-house IT applications in support of a Department or post must establish a local IT CCB.

b. Establish a local IT CCB to ensure that the hardware, software, or network components installed on a LAN do not adversely affect the existing local IT infrastructure under the operational control of bureau/post IT personnel. The local IT CCB must also ensure that all locally approved software and hardware functions only inside the post’s supporting LAN or VLAN segment(s).

c. Local IT CCBS must ensure that the Department’s Information Technology Application Baseline (ITAB) includes current, complete, and accurate data on all general support systems, minor and major applications (see 5 FAH-11 H-014), and other IT resources approved for installation on a Department network; or on IT resources that contain Department data, including websites.
commissioned on behalf of the Department, bureau, office, division, or post.

d. The local IT CCB includes steps in its process for locally approving commercial off the shelf (COTS) IT resources by:

(1) Reviewing industry sources to be specified by the Office of Information Assurance (IRM/IA) concerning vulnerabilities of those IT resources, and correcting any vulnerabilities that pose a threat to the network or Department data as a condition to approval of the software; and

(2) Deciding whether to request and obtain vulnerability scanning of these IT resources by the Bureau of Diplomatic Security as a condition for approval. Thereafter, the local IT CCB must repeat this review and condition process on a recurring basis, supplemented with data on actual configurations from vulnerability and compliance scanning as technically feasible and justified by the level of acceptable risk.

e. The local IT CCB verifies that the local applications' administrators promptly review all vulnerability scanning and configuration compliance data about the locally managed IT resources (provided by the IRM, DS, and/or other Departmental security authorities) to identify and correct vulnerabilities and configuration compliance issues to a level of risk considered acceptable to the Department.

5 FAM 862.2 Local IT CCB Memberships

(CT:IM-145; 07-12-2013)

a. The local IT CCB should consist of a local IT CCB chairperson (i.e., the IMO) and added members as appropriate.

b. For generic information, see the IT CCB website.

5 FAM 862.3 Determining What Must Be Sent to the IT CCB

(CT:IM-145; 07-12-2013)

a. Upon functional area review, if the local IT CCB determines that an application would function outside the local network (or LAN) it must obtain IT CCB approval to use the application.

b. The IT CCB must approve all wireless equipment. The Department does not authorize local IT CCB approval of wireless equipment.

c. The IT CCB must approve all hardware and software used on a classified system.

d. The IT CCB must approve all networked copiers.

e. The IT CCB must approve all multi-functional printers.
f. The IT CCB must approve all network scanners or digital senders.

g. The IT CCB must approve all browsers, ftp, telnet, or CRT software.

h. The IT CCB must approve all modifications to the SOE-D.

i. The IT CCB must approve all convergence of network systems (e.g., systems that consolidate voice, video, and/or data onto the same physical network).

j. See IT CCB website for information on local IT CCB, IT CCB requirements, and membership.

k. All updates to the local IT CCB must be immediately communicated to the IT CCB voting representative.

5 FAM 863 OPERATING SYSTEM SOFTWARE CHANGE CONTROL

(CT:IM-135; 10-10-2012)

a. Only use IT CCB-approved operating systems on the Department’s classified and unclassified networks.

b. The IT CCB will authorize, at most, two versions of PC operating systems, and two versions of server operating systems for use on the Department’s classified and unclassified networks.

c. System administrators must request approval from DS/SI/CS and IRM/IA to use a non-IT CCB-approved operating system. See 12 FAM 623 and 12 FAM 633. For a list of currently approved operating system software, see the IT CCB website.

5 FAM 864 APPLICATION SOFTWARE AND CHANGE CONTROL

(CT:IM-135; 10-10-2012)

a. Implement application software change controls for major and developed applications installed on Department systems:

(1) Define 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) Initiate the systems authorization process;

(3) Test 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 and authority to operate process);

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

(5) Limit access to software programming libraries;
(6) Protect system documentation, as appropriate, with the same due diligence as the data that are protected; and
(7) Operate the IT CCB-approved SOE without negative impact to other SOE components.

b. Each system owner must ensure the 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.

c. The Department IT CCB or the local IT CCB must approve each application, as appropriate, before it is used. See 5 FAM 862.3.

d. All government-off-the-shelf (GOTS) or commercial-off-the-shelf (COTS) applications need to be contained in the Information Technology Application Baseline (ITAB). Posts and bureaus are responsible for ensuring that any applications they develop or purchase are already present or are added to the ITAB. See the ITAB website for instructions on adding and/or updating information.

5 FAM 865 COPYRIGHTED SOFTWARE

(CT:IM-135; 10-10-2012)

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

b. The Sourcing Management Division (IRM/BMP/GRP/SM) manages the enterprise software licensing agreements for the Department. (See 5 FAM 915.11-1, paragraph e.)

c. The IMO/ISO/System Administrator must install copyrighted software in order to conform with the Department’s enterprise licensing agreements, or locally approved licensing agreements.

d. The IMO/ISO/System Administrator must inform IRM/OPS/ENM/NLM/ITA of locally approved licensing agreements or locally funded versions of any IT CCB-approved software.
5 FAM 866 PATCH MANAGEMENT

(CT:IM-145; 07-12-2013)

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. The Software Lifecycle Management (IRM/OPS/ENM/PSD/SLM) Branch manages the Department’s Enterprise Patch Management Program.

c. IMOs/ISOs/system administrators must follow guidelines 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.

e. The Enterprise Patch Management Program will only patch the newest versions of approved software products within its scope.

f. All Departmental application owners and/or developers must designate a person or group to represent their organization in the Patch and Vulnerability Group (PVG). There are two purposes of the PVG:

   (1) To champion patch management compliance in their respective organizations; and

   (2) To test patches as they are released against their functional applications and provide testing results to the Enterprise Patch Management Program.

5 FAM 867 DOCUMENTATION

(CT:IM-145; 07-12-2013)

System managers/system owners must maintain documentation for all aspects of computer support and operations. This documentation is important to ensure continuity and consistency throughout the Department. 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 standalones), printers, servers, and other network peripherals/devices (e.g., scanner), the office in which each is located, the cable number/device serial 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 IT system performance report (i.e., capacity, availability, integrity, etc.);

(6) A systems operations log. You must maintain this log for 6 months. (See 12 FAM 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 6 consecutive months; and

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

5 FAM 868 AND 869 UNASSIGNED