

5 FAM 800 INFORMATION SYSTEMS MANAGEMENT

5 FAM 810 INFORMATION SYSTEMS MANAGEMENT

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

5 FAM 811 GENERAL

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

This chapter establishes policies for operating and managing IT operating environments abroad and domestically in the Department of State. It applies to all personnel involved with the IT lifecycle for all systems, software controls, contingency plans, hardware and software maintenance, networks, data integrity, and logistical access controls.

5 FAM 812 SCOPE

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

The chapter discusses responsibilities, IRM InfoCenter, software controls, continuity of operations, hardware and software maintenance, and networks.

5 FAM 813 AUTHORITIES

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

The authorities for these policies and procedures are

- (1) Paperwork Reduction Act of 1995, Public Law 104-13, 44 U.S.C. ch. 35;
- (2) Information Technology Management Reform Act of 1996; (ITMRA)(Clinger-Cohen Act); Public Law 104-106;

- (3) OMB Circular A-130, revised November 28, 2000;
- (4) Presidential Decision Directive (PDD) 63, May 22, 1998;
- (5) Federal Acquisition Regulation (FAR), Part 39, 48 CFR Part 39;
- (6) Government Performance and Results Act of 1993, Public Law 103-62;
- (7) Federal Information Security Management Act (FISMA), (Pub. L. 107-347, Title III); and
- (8) OMB Quality of Information Guidelines, 67 FR 8451-8460 (Feb. 22, 2002).

5 FAM 814 DEFINITIONS

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

- a. **Authorization.** The formal approval of an IT system to process, store, or transmit information granted by a management official. Authorization, which is required under OMB Circular A-130, is based on an assessment of the management, operational, and technical controls associated with an IT system.
- b. **Certification.** The comprehensive evaluation of the technical and non-technical security controls of an IT system to support the authorization process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.
- c. **ClassNet.** A physical and logical Internet Protocol (IP) based global network that links the Department of State's domestic sites and embassies, consulates, and annexes abroad for communications up to and including the Secret level of classification.
- d. **Cyber Security.** Information operations that protect and defend information and IT systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IT systems by incorporating protection, detection, and reaction. (Definition source: Systems Authorization Plan)
- e. **Dedicated Internet Network (DIN).** Dedicated Internet access from an Internet Service Provider (ISP) on a discrete local area network (LAN) that is not connected to any other Department system. Abroad, DINs are called Overseas Dedicated Internets (ODIs).

- f. **Designated Approval Authority (DAA).** The person formally authorized to assume responsibility for operating a system at an acceptable level of risk. For the Department, the Chief Information Officer (CIO) is the DAA, except in the case of SCI, see IRM 1 FAM. This term is synonymous with designated accrediting authority and delegated accrediting authority.
- g. **Information Technology Systems (IT Systems).** A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with procedures, whether automated or manual. (Definition source: OMB Circular A-130)
- h. **Information Systems Security Officer (ISSO).** The person responsible to the system/data owner for ensuring the security of an IT system throughout its lifecycle, from design through disposal. (Definition Source: Systems Authorization Plan).
- i. **Information Technology Application Baseline (ITAB).** The repository for information on all Department applications. This is the official source of external reporting regarding the Department's application portfolio.
- j. **Information Technology Change Control Board (IT CCB).** The entity that manages hardware, software, and hardware/software configuration changes to the Department's global IT environment. The IT CCB has responsibility for changes that potentially affect the Department's global IT environment. The scope includes unclassified, Sensitive But Unclassified (SBU), and classified infrastructures (stand-alone or networked) up to and including the Secret level of classification.
- k. **Local Area Network (LAN).** A number of interconnected data communication protocols and devices joining a wide variety of devices such as computers, printers, storage devices, and other peripheral equipment within a single building or a campus of buildings. LANs provide the capability to share files and other resources among multiple users.
- l. **Local Change Control Board (Local CCB).** A formally constituted group of stakeholders responsible for maintaining control of their own change processes.
- m. **OpenNet.** A physical and logical Internet Protocol (IP) based global network that links the Department's domestic sites and embassies, consulates, and annexes abroad at the unclassified or sensitive but unclassified level.

- n. **Risk Management.** The total process of identifying, controlling, and mitigating IT system-related risks. It includes risk assessment; cost benefit analysis; and the selection, implementation, test, and security evaluation of security controls. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws. (Definition Source: Systems Authorization Plan)
- o. **Stand-alone.** A device that functions independently of a network.
- p. **Support System.** An interconnected set of information resources under the same direct management control and sharing common functionality.
- q. **System Authorization Plan (SAP).** A comprehensive and uniform approach to the System Authorization Process that is comprised of four phases: Phase 1 – Precertification; Phase 2 – Certification; Phase 3 – Authorization; and Phase 4 – Post-Authorization.
- r. **System Owner.** The Bureau Executive is the owner of locally developed systems at the post or bureau level responsible for the IT system during initial development and acquisition. The System Owner is concerned with cost, schedule, and performance issues for the system as well as security issues and represents the interests of the user community and the IT system throughout the system lifecycle. (Definition Source: Systems Authorization Plan)
- s. **Unauthorized Disclosure.** The release of password information to persons other than senior IT management or security personnel for purposes of performing an investigation
- t. **Universal Trouble Ticket (UTT).** An incident/problem reporting and tracking system designed for use by multiple Department action offices. Each action office operates within a tier structure. The IRM InfoCenter is the Tier I action office receiving the majority of trouble calls. Tier I action officers create UTT tickets and transfer tickets they cannot resolve to Tier II/III action offices. Tier II/III action offices provide skilled technical support in specific areas.
- u. **Wide Area Network (WAN).** A data communication function that connects geographically disparate Local Area Networks using long-haul networking facilities and protocols.

5 FAM 814 THROUGH 819 UNASSIGNED