

5 FAM 820 INFORMATION TECHNOLOGY ROLES AND RESPONSIBILITIES FOR SYSTEM OPERATIONS/MANAGEMENT

(Office of Origin: IRM/APR/RG)

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

5 FAM 821 GENERAL

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

This section defines responsibilities for system operations and management. See also 5 FAM 120, 12 FAM 622, and 12 FAM 630.

5 FAM 822 CHIEF INFORMATION OFFICER

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

- a. Is the Department's Senior Information Technology professional. The CIO reports via the Undersecretary for Management to the Secretary of State on all matters relating to Information Resource Management;
- b. Ensures availability of information technology systems and operations, including IT contingency planning, to support the Department's diplomatic, consular, and management operations;
- c. Ensures that appropriate procedures are in place for system authorization of national security systems; and
- d. Serves as the Designated Approval Authority (DAA) for non-Special Compartmented Information (non-SCI) systems in the Department.

5 FAM 823 CHIEF INFORMATION SECURITY OFFICER (CSIO)

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

- a. Reports directly to the CIO on all matters pertaining to IT security;
- b. Develops and maintains the Department's information security program;
- c. Provides guidance to personnel with responsibilities for information security and liaison with Information Systems Security Officers (ISSOs) domestically and abroad; and
- d. Coordinates the design and implementation of processes and practices that assess and quantify risk.

5 FAM 824 INFORMATION SYSTEMS SECURITY OFFICERS (ISSOs)

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

- a. Ensure systems for which they are responsible are configured, operated, maintained, and disposed of in accordance with all relevant IRM and DS security guidelines;
- b. Are responsible for overseeing configuration and administration of auditing and for ensuring that audit trails are reviewed periodically and archived in accordance with security guidelines;
- c. Work closely with IMO/ISO/System Administrator to ensure all security related functions and activities are performed;
- d. Play a leading role in introducing an appropriate methodology to help identify, evaluate, and minimize risks to all IT systems; and
- e. Are responsible to the CISO to ensure that IT system is configured and maintained securely throughout its lifecycle in accordance with the Systems Authorization Plan (SSP). See also 12 FAM 620 and 12 FAM 630.

5 FAM 825 SYSTEM OWNER

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

a. Domestically, the System Owner is the bureau designated senior executive that is responsible for the system. Abroad, the System Owner is the Charge, Deputy Chief of Mission, Consul General, or Principal Officer or equivalent, or the bureau designated senior executive responsible for the system.

b. Each System Owner:

- (1) Is responsible and accountable for the business aspects of managing a system, including funding and representing the interests of the system throughout its lifecycle;
- (2) Ensures adequate confidentiality, integrity, and availability of data and applications software residing on the system;
- (3) Ensures system security plans and contingency plans are developed and maintained for each system and applications; and
- (4) Ensures systems personnel are properly designated, and trained; and appoints the Information System Security Officer (ISSO) and the alternate ISSO for a system.

5 FAM 826 INFORMATION MANAGEMENT OFFICER (IMO)/INFORMATION SYSTEMS OFFICER (ISO)/SYSTEM ADMINISTRATOR

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

The IMO/ISO/System Administrator:

- (1) Develops and maintains system security plans and contingency plans for all IT systems and major applications for which he or she is responsible;
- (2) Participates in risk assessments to periodically reevaluate sensitivity of the system, risks, and mitigation strategies; and
- (3) Installs only hardware and/or software approved by the IT CCB or Local CCB. See 5 FAM 120 for further information on the roles and responsibilities of personnel managing systems abroad.

5 FAM 827 USER

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

The user must:

- (1) Adhere to Department guidelines governing the personal use of information systems;
- (2) Not download, install, or use software on any Department computer without prior approval from the Information System Security Officer (ISSO) or ISSO's delegated representative;
- (3) Use e-mail systems in a professional and courteous manner with the understanding that misuse of Department e-mail will subject them to disciplinary action (see 12 FAM 642);
- (4) Use properly formatted passwords and protect them from unauthorized disclosure. Unauthorized disclosure is the release of password information to persons other than senior IT management or security personnel for purposes of performing an investigation; and
- (5) Not use a system or application before receiving appropriate training.

5 FAM 828 THROUGH 829 UNASSIGNED