12 FAM 630
CLASSIFIED AUTOMATED INFORMATION SYSTEMS

(TL:DS-83; 10-07-2002)

12 FAM 631 PERSONNEL SECURITY

(TL:DS-69; 06-22-2000)

a. The Department establishes personnel security procedures which require that all employees accessing any of the Department's classified automated information system (AIS) processing resources have the following:

(1) A Secret security clearance at a minimum;

(2) The appropriate access levels and need to know in connection with the performance of official duties; and

(3) Knowledge of their AIS security responsibilities.

b. Policies and procedures that appear in this section implement the personnel security program for all of the Department's classified AISs, both domestic and abroad.

12 FAM 631.1 Security Clearances

12 FAM 631.1-1 Domestic

(TL:DS-69; 06-22-2000)

a. The data center manager, the system manager and the ISSO must ensure that all personnel with system administrator privileges to an AIS processing classified information and connected to a communications system have a Top Secret security clearance.

b. The data center manager, the system manager and the ISSO must ensure that all personnel with access to classified AISs have a Secret security clearance at a minimum. Secret-cleared personnel may access an AIS connected to an AIS/communications system processing Top Secret information provided DS-approved hardware and software control mechanisms prevent such personnel from accessing Top Secret information.

12 FAM 631.1-2 Abroad

(TL:DS-69; 06-22-2000)

a. The regional security officer (RSO) or post security officer (PSO) must ensure that all personnel with system administrative access to an AIS processing classified information and connected to a communications processor have a Top Secret security clearance.

b. The RSO must ensure that all personnel with access to classified AISs have a Secret security clearance at a minimum. Secret cleared personnel may access an AIS connected to an AIS/communications system processing Top Secret information provided DS-approved hardware and software control mechanisms prevent such personnel from accessing Top Secret information.

12 FAM 631.2 Personnel Management

12 FAM 631.2-1 Security Responsibilities Statement

(TL:DS-69; 06-22-2000)

Supervisors must include a statement specifying responsibilities for AIS security in job and work requirements statements for computer operations staff and program managers who have responsibility for specific applications.

12 FAM 631.2-2 Separation of Duties

(TL:DS-83; 10-07-2002)

a. The data center manager, the system manager and the user's supervisor must configure user access privileges to ensure that users receive access only to the information and system functionality required to perform their official duties. Access privileges must be consistent with the separation of duties for handling classified information established in 12 FAM 500 for manual processes.

b. Supervisors must annually review access privileges of each application user under their supervision to verify that the privileges originally granted are still appropriate. The data center manager and the system manager will provide supervisors with any information necessary to aid in the review and retain written documentation of directed changes.

c. See 12 FAM *637* for additional information.

12 FAM 632 ADMINISTRATIVE SECURITY

12 FAM 632.1 Management Control Process

12 FAM 632.1-1 TEMPEST

(TL:DS-69; 06-22-2000)

a. All facilities processing classified information and or unclassified information in the highest threat environments will employ TEMPEST countermeasures in proportion to the risk of exploitation and the associated potential damage to the conduct of foreign relations and national security. Abroad, each mission must state who is responsible for maintaining TEMPEST security (e.g., RSO, IMO, ISSO, etc.).

b. Approval for the use of non-TEMPEST equipment must be requested from the Department's Certified TEMPEST Technical Authority (CTTA).

c. The data center manager and the system manager must ensure that TEMPEST AIS components are not inadvertently interchanged with components from non-TEMPEST AISs. Only with CTTA approval is the connection of TEMPEST and non-TEMPEST equipment permitted.

12 FAM 632.1-2 Appointment of an Information Systems Security Officer (ISSO)

(TL:DS-69; 06-22-2000)

a. For each Department AIS, an ISSO must be designated, in writing, to manage the AIS security program. An alternate ISSO must also be designated, in writing, to fulfill these duties in the absence of the ISSO. These requirements apply regardless of the size of the AIS. For nonmainframe AISs, these designations will be made by the executive director for each bureau or office for a domestic AIS, and by the administrative officer for an AIS abroad. For mainframe AISs, these designations will be made by the data center manager in consultation with the Mainframe Security Program manager. For RIMC AISs, these designations will be made by the RIMC Director. 12 FAM 632 Exhibit 632.2-1 contains a sample memorandum assigning ISSO responsibilities to an individual.

b. On nonmainframe AISs, the ISSO and alternate ISSO do not have to be system managers. On mainframe AISs, the duties of the ISSO and alternate ISSO must be separate from those of the data center manager.

c. On nonmainframe AISs, the ISSO and the alternate ISSO will

have full access to the AIS. On mainframe AISs, the ISSO and alternate ISSO will be given access to only those system functions that are required for them to perform their official duties. Additionally, on mainframe AISs where the central components of a classified distributed AIS are located within the information programs center (IPC), the ISSO and alternate ISSO must also have crypto clearances for use.

d. In compliance with the Department's Internal Controls Program, the ISSO's performance appraisal will be based in part on effective implementation of AIS security requirements. See 12 FAM 638 for additional information.

e. For mainframe AISs, a copy of the signed memorandums designating the mainframe application ISSO and the alternate mainframe application ISSO must be submitted to IRM/OPS/ITI/SI.

f. IRM/OPS/ITI/SI shall designate, in writing, a Mainframe Security Program manager who will implement and manage the Department's AIS security program for mainframe AISs. The Mainframe Security Program manager will advise all mainframe application ISSOs on the Department's mainframe AIS security policies and procedures so that no one mainframe AIS will compromise the security of another. He or she will also facilitate the exchange of information among mainframe ISSOs and will assist them in solving technical or procedural problems. IRM/OPS/ITI/SI shall designate, in writing, an alternate Mainframe Security Program manager to fulfill those responsibilities when the primary Mainframe Security Program manager is absent.

12 FAM 632.1-3 Controlling Access to Systems

(TL:DS-69; 06-22-2000)

a. The ISSO, on mainframe AISs, and the system manager, on nonmainframe AISs, must control and limit AIS access to the level necessary for users to perform their official duties.

b. Supervisors must complete a system access request for each authorized user.

c. Personnel officers must include the data center manager and the system manager on the bureau or post checkout list to ensure timely notification of all employees and contractors who are transferred or terminated. The data center manager and the system manager, in conjunction with the ISSO, must revoke user access privileges for these personnel. Personnel officers must notify the data center manager, system manager, RSO, and ISSO promptly of any employee or contractor with system access who is terminated for cause. Revocation of user access privileges is immediate.

d. The ISSOs on nonmainframe AISs will annually review all AIS users with exceptional access privileges. The ISSOs on mainframe AISs will review at least quarterly all AIS users with exceptional access privileges. These reviews will be accomplished to ensure that such privileges are needed in order for the users to perform their official duties.

e. The program manager must annually review the access privileges for each AIS mainframe user with access to an application system/database under the user's supervision to ensure that the access is still needed in order for the user to perform his or her official duties. The program manager shall report the findings of the review to the appropriate ISSO.

f. When a mainframe AIS application system/database is being accessed by other application systems or by other independent processes, the program manager responsible for the application system/database must annually review these accesses to ensure that the access is still needed in order for the other application system or independent process to perform its function. The program manager shall report the findings of the review to the appropriate ISSO.

g. The ISSO, on mainframe AISs, must ensure that contractor personnel, who have been granted mainframe AIS access retain this access for only a specified period of time, not to exceed three years. At the end of the specified time period, contractor personnel must make a formal request to the ISSO for their AIS access to be renewed.

12 FAM 632.1-4 Password Controls

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager must initially assign each new user a minimum three-character user ID and a minimum six-to-eight character, alphanumeric, randomly generated password. Once the new user has accessed the system for the first time, the user must then change this issued password within ten calendar days, creating a new password according to these specifications:

(1) Password length. The password must be a minimum of eight characters in length. If the system which the user is accessing does not accommodate eight characters, then the user should use the maximum number of character spaces available;

(2) Password composition. The password must be composed of characters from at least three of the following four groups from the standard keyboard:

(a) Upper case letters (A-Z);

(b) Lower case letters (a-z);

(c) Arabic numerals (0 through 9); and

(d) Nonalphanumeric characters (punctuation symbols);

(3) Thereafter, users should construct their own passwords when required: at least once every six months, and when it is suspected that the password has been compromised. The latter must also be reported to the ISSO.

b. For AISs that cannot be configured to filter user-created passwords, it is acceptable for data center managers and system managers to issue machine-generated passwords to users. Any data center manager or system manager without a means to produce machine-generated passwords to distribute may obtain them from IRM/OPS/ITI/SI.

c. Passwords to network devices (e.g., switches, routers) should be constructed and issued as stated in paragraph a of this section or as in paragraph b of this section when the password construction in paragraph a cannot be accommodated.

d. The data center manager and the system manager may not maintain permanent user IDs and passwords on AISs for visitors, training, demonstrations, or other purposes.

e. If distributing passwords to users, the data center manager and the system manager must act in a manner which prevents disclosure to other individuals, and advise users of the password's classification. PASSWORDS WILL BE CLASSIFIED AT THE HIGHEST LEVEL OF CLASSIFIED INFORMATION FOR WHICH THE SYSTEM IS AUTHORIZED, AND, THEREFORE, THE SAME PASSWORDS MAY NOT BE USED FOR UNCLASSIFIED SYSTEMS. Users must inform the ISSO if they suspect compromise of their passwords.

f. Users must acknowledge receipt of their user IDs and passwords by signing password receipts/security acknowledgements. See 12 FAM 629 Exhibit 629.2-2a for a sample format.

g. The data center manager and the system manager must ensure that all passwords are changed under the following conditions:

(1) At least once every six months;

(2) Immediately following any suspected compromise; or

(3) Whenever someone with system security authority no longer requires that level of access.

To ensure that all passwords are changed every six months, the data center manager and the system manager should either use a tickler file, or preferably, reconfigure the AIS to require the user to create a new password to maintain access to the AIS after six months.

h. The data center manager and the system manager must immediately delete individual user IDs and passwords under the following conditions:

(1) Whenever a user's supervisor determines the user no longer requires systems access;

(2) Whenever notified by a proper authority, such as the personnel officer, that the user's employment has been terminated with the Department or that the user has transferred to another office or post;

(3) Whenever notified by the Bureau of Diplomatic Security that a user's security clearance has been suspended or revoked; or

(4) Whenever requested by proper investigative authority or by the supervisor at the request of proper investigative authority pursuant to a criminal or national security investigation.

12 FAM 632.1-5 Use of Systems

(TL:DS-83; 10-07-2002)

a. The ISSO must notify all AIS users that personal use of the Department's classified AIS equipment is strictly prohibited; therefore, users do not have a reasonable expectation of privacy in the AIS. The Director, Diplomatic Security Service, may authorize access to special agents of the Department of State and other Federal law enforcement agencies in the conduct of investigations concerning employee misconduct or the violation of any Federal law. See 12 FAM 637 for additional information.

b. The ISSO must instruct all AIS users that classified workstations are never to be left unattended when logged on. All activity occurring when the workstation is functioning is the responsibility of the logged-on user. See 12 FAM 637 for additional information.

c. The ISSO, data center manager or system manager must ensure that DS-approved labels, indicating the highest level of information processed by the AIS, are affixed to all classified AISs.

d. Users must process NODIS and EXDIS information under the most stringent access controls available on the AIS. NODIS and EXDIS information should remain on the AIS only a minimal amount of time. Users must inform the data center manager and the system manager when NODIS and EXDIS information is placed on the AIS. NODIS and EXDIS

information should be purged from the AIS as soon as it is no longer needed.

e. Mainframe AIS users must also comply with established mainframe operational procedures and guidance issued by IRM/OPS/ITI/SI.

12 FAM 632.1-6 Protection of Media and Output

(TL:DS-83; 10-07-2002)

a. The data center manager and the system manager must instruct users to protect all media used on, and all hard copy material generated by, classified AISs according to 12 FAM 500 which defines requirements for marking, classifying and declassifying, accountability, transportation, transmission, storage, and destruction of national security information.

b. The data center manager and the system manager must limit access to the operating system and application software designated for use on the classified AIS to U.S. citizen personnel who are cleared and authorized access. The data center manager and the system manager must store all operating system and application software in an approved security container. See 12 FAM 637 for additional information.

c. Abroad, the RSO or PSO must review and approve all locally established procedures for transportation and control of classified media. Media shipped between posts must be sent by classified pouch. See 12 FAM 500 for domestic transportation requirements.

d. AIS users must review all hard copy output prior to relaxing the controls relating to processing classified information. All output must be handled as if classified at the highest classification processed on the AIS. Classification will remain unchanged until reviewed by an individual cleared to the same level.

e. AIS users must mark all removable magnetic media to indicate the highest classification level of information authorized to be processed on the AIS. All media will be handled as required by the labels.

f. Only media which has been shipped via classified pouch and under the continuous control of cleared U.S. citizens may be loaded onto an AIS-approved for classified processing. See 12 FAM 637 for additional information.

12 FAM 632.1-7 Security Incident Procedures

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager documents, in the operations log, all security-related abnormal system operations such as

unexplained changes in user or program access privileges, improper system responses to access control processes, or other hardware or software failures that may result in unauthorized disclosure, loss, or modification of system programs or data.

b. The data center manager and the system manager must immediately notify the following of any security-related abnormal system operation:

(1) ISSO;

(2) The RSO or PSO (if abroad);

(3) DS/CIS/IST;

(4) IRM/OPS/ITI/SI or regional information management center (RIMC); and

(5) The regional computer security officer (RCSO), if applicable.

c. Any AIS user discovering or suspecting incidents of fraud, misuse, unauthorized disclosure of information, destruction or unauthorized modification of data, or unauthorized access attempts must immediately report the incident to the ISSO or RSO or PSO. The ISSO, data center manager and system manager must provide the RSO or PSO with technical assistance and advice if an investigation is required.

d. If an incident indicates unauthorized disclosure, modification, destruction, or misuse of AIS resources, the data center manager and the system manager must immediately make a full backup copy of the AIS for review. Domestically, the ISSO must report these events to appropriate Department application developers and DS/CIS/IST. Abroad, the ISSO must report these events to the RSO or PSO, appropriate Department application developers, the RCSO or RIMC, DS/CIS/IST, and IRM/OPS/ITI/SI via telegram. The ISSO must make the AIS backup available for review and provide the RSO or PSO with technical assistance and advice if an investigation is required. If necessary, the ISSO may order that all AIS operations be halted.

12 FAM 632.1-8 Violations and Infractions

(TL:DS-69; 06-22-2000)

a. Individuals who do not comply with AIS policies and procedures will be subject to the violations and infractions regulations contained in 12 FAM 500.

b. Domestically, the ISSO must notify DS/ISP/APB. Abroad, the RSO or PSO and ISSO must investigate all known or suspected incidents

of noncompliance with the provisions of this subchapter and inform post management of the results.

c. The ISSO reviews randomly selected user libraries and PC hard disk drives and floppies to ensure that users are not processing information classified above the level that is authorized for the AIS.

12 FAM 632.1-9 Disposition of Media, Output, and Equipment

(TL:DS-83; 10-07-2002)

a. AIS users must destroy classified hardcopy output when no longer needed by incineration or shredding.

b. The data center manager, system manager and ISSO must ensure that magnetic storage media used on classified AISs is not removed from U.S. Government-controlled premises for any reason, including maintenance, credit, or sale. Media which has been used on a classified AIS may not be returned to the vendor for credit. Such media may only be used on another AIS authorized to process classified information.

c. Abroad, the data center manager and the system manager must forward all damaged classified hard magnetic media (fixed disks, disk cartridges, or disk packs) to IRM/OPS, for disposition. Domestically, the data center manager and the system manager must forward all damaged classified hard magnetic media (fixed disks, disk cartridges, or disk packs) to IRM/OPS, for disposition. See 12 FAM 637 for additional information.

d. The data center manager and the system manager must destroy soft types of damaged, obsolete, or excess classified magnetic media (i.e., diskettes and tapes) by burning or disintegration.

e. Used laser toner cartridges may be treated, handled, and stored as UNCLASSIFIED material. See 12 FAM 539.5-3 for additional information.

12 FAM 632.1-10 System Maintenance

(TL:DS-83; 10-07-2002)

a. Users must not tamper with TEMPEST equipment in any way. Abroad, only Top Secret-cleared personnel who are authorized access to the equipment may perform system maintenance. Domestically, only authorized maintenance personnel who are cleared to the highest level of information processed or stored on the AIS may perform maintenance on that system. AISs connected to a communications processor must be maintained by Top Secret-cleared maintenance personnel. See 12 FAM 637 for additional information.

b. The data center manager and the system manager must ensure that maintenance personnel do not remove any magnetic media ever mounted onto a classified AIS.

c. The data center manager and the system manager will ensure that a maintenance log documents all maintenance or service performed on the AIS. See 12 FAM 637 for additional information.

12 FAM 632.1-11 Review of Audit Logs

(TL:DS-83; 10-07-2002)

a. The ISSO will generate and review audit logs at least once a month. See 12 FAM 637 for additional information. The ISSO may select additional activities for review based on type of information processed.

b. The ISSO informs the data center manager, the system manager and, abroad, the RSO or PSO, of all security-related anomalies discovered during the review of audit trails.

12 FAM 632.2 Training

(TL:DS-83; 10-07-2002)

a. DS/PLD/TC provides AIS security training to ISSOs, data center managers, system managers, and other Department personnel who have security responsibilities for Department classified AISs. DS/PLD/TC provides AIS security awareness and training materials. See 12 FAM 637 for additional information.

b. Department organizations developing software and systems for use abroad must include AIS security awareness training and familiarization with Department policies and procedures for personnel involved in the process.

c. IRM/OPS/ITI/SI will provide mainframe AIS security utility software training to mainframe ISSO's. When necessary, IRM/OPS/ITI/SI will also provide this training to mainframe end users.

d. Domestically, the ISSO, and abroad, the RSO, in conjunction with the ISSO, the data center manager and the system manager, must ensure that all personnel with access to systems have received site-specific AIS security training.

12 FAM 632.3 Backup and Contingency Planning

12 FAM 632.3-1 Backup

(TL:DS-69; 06-22-2000)

a. The system manager shall implement and document a full backup procedure for system programs and information to ensure continuity of operations.

b. For all nonmainframe AISs administered by the Department of State, the system manager must place a password with security administrator privileges in a sealed envelope and give it to the executive director, domestically, and, abroad, to the RSO, IMO, and administrative officer for availability under emergency situations or exceptional conditions. Domestically, the executive director, and abroad, the RSO, IMO, and administrative officer must ensure that this password is stored in a secure location. The system manager will notify the ISSO and IMO in writing if this password is used under emergency or exceptional conditions and will issue a new password for the backup ID.

c. On mainframe AISs administered by the Department of State, IRM/OPS/ITI/SI must place a firecall (emergency) password with security administrator privileges in a sealed envelope and provide it to the data center manager for availability under emergency situations or exceptional conditions. The data center manager must ensure that the firecall password is stored in a secure location. The data center manager will notify the mainframe ISSO and IRM/OPS/ITI/SI in writing if the firecall password is used. IRM/OPS/ITI/SI will then issue a new firecall password to the data center manager.

d. AISs administered by U.S. Government agencies other than the Department of State will comply with the backup and contingency planning requirements of the responsible agency.

e. PC users must periodically backup their data onto floppy diskettes to ensure continued operations. Users must store their backup data in an approved security container within a controlled access area (CAA) abroad or within a facility authorized to store or process classified information domestically, but as far away as possible from the PC. Distance minimizes the potential for complete loss of programs and data should a major catastrophe occur.

f. The data center manager and the system manager must ensure that all backup media is appropriately labeled to indicate the highest level of classified information processed on the AIS.

g. The data center manager and the system manager must store

backup media for distributed AISs in an approved security container. The storage location must be within the CAA abroad or within a facility authorized to store or process classified information domestically, but as far away as possible from the main processing center. Distance minimizes the potential for complete loss of programs and data should a major catastrophe occur. The data center manager and the system manager make certain that alternate storage locations are protected from adverse environmental conditions, such as extreme heat, humidity, and air pollution.

12 FAM 632.3-2 Contingency Plan Preparation

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager are responsible for developing a contingency plan for all classified AISs.

b. The data center manager, system manager and RSO or PSO will coordinate the contingency plan with the post emergency action plan. Any emergency response procedures specified in the contingency plan must be consistent with the post emergency action plan.

c. The data center manager and the system manager update each contingency plan annually, or when major modifications to the AIS occur. The data center manager and the system manager should test each contingency plan annually, or when major modifications are made.

12 FAM 632.4 Security Plan Preparation

12 FAM 632.4-1 General Support Systems

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager, in conjunction with the ISSO, are responsible for developing a security plan for all general support systems under their control. (A general support system is defined as an interconnected set of information resources under the same direct management control which shares common functionality.)

b. The data center manager and the system manager, in conjunction with the ISSO, update each general support system security plan annually or when major modifications to the general support system occur.

c. The data center manager and the system manager, in conjunction with the ISSO, will ensure that IRM/OPS/ITI/SI receives a copy of the general support security plan and any updates to the general support security plan for retention in a central repository of such plans.

12 FAM 632.4-2 Major Application Systems

(TL:DS-69; 06-22-2000)

a. The program manager, in conjunction with the data center manager, system manager and ISSO, is responsible for developing a security plan for each major application system under his or her control. (A major application is defined as an application that requires special management oversight and attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.)

b. The program manager, in conjunction with the data center manager, system manager and ISSO, updates each major application system security plan annually or when major modifications to the major application system occur.

c. The program manager, in conjunction with the data center manager, system manager and ISSO, will ensure that IRM/OPS/ITI/SI receives a copy of the major application system security plan and any updates to the major application system security plan.

12 FAM 632.5 Log and Record Keeping

(TL:DS-69; 06-22-2000)

a. The ISSO, on nonmainframe AISs, and IRM/OPS/ITI/SI on mainframe AISs ensure that the following logs and records are maintained for all facilities:

(1) System access requests;

(2) Password receipts/security acknowledgements;

(3) System maintenance logs;

(4) Audit trail logs; and

(5) System operation logs.

b. The data center manager and the system manager must maintain all logs for at least six months, with the exception of password receipts/security acknowledgements, which shall be kept for the duration of the user's access to that AIS and for six month's after the user's departure.

12 FAM 633 SYSTEMS IMPLEMENTATION

(TL:DS-69; 06-22-2000)

Due to variations in hardware and software capabilities between different AISs, post personnel must implement the controls described below that are applicable to their specific AIS.

12 FAM 633.1 Operating System and Application Software

(TL:DS-83; 10-07-2002)

Citizens of countries for which DS/DSS/ITA has assessed a critical technical and/or human intelligence threat level shall not develop, modify, or perform maintenance on software used on Department of State computer systems, unless there has been specific DS authorization for each incidence. The information management officer (IMO) responsible for State Department computer systems, both domestically and abroad, must obtain DS/CIS/IST/ACD authorization before such work is begun. See 12 FAM 637.3-4 for procedures on obtaining such approval.

12 FAM 633.1-1 Operating System Software

(TL:DS-69; 06-22-2000)

a. Abroad, the data center manager and the system manager ensure that all classified AISs use only the Department-approved and distributed version of the vendor operating system. IRM will distribute all operating system software to post via classified pouch. Domestically, the data center manager and the system manager ensure that DS/CIS/IST is notified prior to installing operating system software that has never before been installed on any Department multi-user AIS.

b. Only the data center manager and the system manager may install new releases, upgrades, or patches to the vendor operating system. If abroad, these must be received from the Department. Abroad, software sent directly by a vendor or a vendor's authorized distributor will not be installed on any post AIS without prior IRM approval.

c. AIS users must not modify operating system software.

d. The data center manager and the system manager must control access to all system software, utilities, and functionality that could be used to gain unauthorized access to application data and program code. The data center manager and the system manager will restrict such access to the minimum number of authorized users required to perform their official

duties.

e. On domestic mainframe AISs and on mainframe AISs abroad, system staff members must not modify operating system software except when installing or applying Department approved and distributed software updates or fixes. The data center manager must approve all such updates.

f. On domestic mainframe AISs and on mainframe AISs abroad, whenever operating system software is installed for which access control is an optional or add-on component, the ISSO in conjunction with IRM/OPS/ITI/SI and the mainframe AIS staff must ensure that the access control component or add-on program is installed simultaneously with the operating system software.

g. On domestic mainframe AISs and on mainframe AISs abroad, system staff members must not install software products which introduce supervisor calls (SVCs), appendages, authorized programs, interfaces for logging on, facilities for submitting jobs for execution or methods of accessing or transferring data without first ensuring that the products correctly interface with the system security software (e.g., ACF2) and will not adversely affect the security posture of the AIS. The ISSO must ensure that IRM/OPS/ITI/SI and DS/CIS/IST are notified in writing in the event that these requirements cannot be met with respect to any software program product residing on the AIS.

h. On domestic mainframe AISs and on mainframe AISs abroad, the ISSO, in conjunction with IRM/OPS/ITI/SI, must ensure that periodic integrity checks are performed on the mainframe AIS so that:

(1) All vendor-supplied updates or fixes have been reviewed and do not compromise the integrity of the AIS;

(2) All Department programs and routines have been reviewed and do not compromise the integrity of the AIS; and

(3) All new operating systems have been reviewed and do not compromise the integrity of the AIS.

All findings should be reported to the data center manager, IRM/OPS/ITI/SI and DS/IST/ACD

12 FAM 633.1-2 Application Software

(TL:DS-69; 06-22-2000)

a. Abroad, the data center manager and the system manager ensure that only Department-approved and distributed versions of application software are used on classified AISs. All Department application software must be sent to posts via classified pouch. Cognizant post officials who

have identified a need for special application software may approve its use and procure it through approved Department channels. Domestically, only data center managers and system managers may load versions of software to be used on classified AISs.

b. Department and contractor personnel, other than authorized application developers, may not modify Department standard application software.

c. Domestically, Department personnel may develop application software, provided that it is developed and documented in accordance with applicable Department standards. All internally developed application software provided to other offices must remain under Department control during transport or be shipped by U.S. registered mail.

d. Abroad, the data center manager and the system manager ensure that all new releases, upgrades, or patches to Department application software installed on post AISs have been approved by and received from the Department.

e. The data center manager and the system manager must ensure that users' access rights and privileges are consistent with functional responsibilities and authorities. Access must be based on need to know, least privilege, and supervisory requirements.

f. The data center manager and the system manager ensure that privately owned, shareware, or bulletin board software is not installed or processed on U.S. Government AISs.

g. The data center manager and the system manager ensure that all application software is acquired in accordance with Federal copyright laws.

h. The executive director for each bureau or office sponsoring a mainframe AIS application system or database must designate in writing a program manager for each such application system or database.

i. For each Department-sponsored mainframe AIS application system or database, a protection schema must be developed. A protection schema is an outline detailing the types of access users may have to a database or application system, given the user’s need-to-know, e.g., read, write, modify, delete, create, execute, and append. This protection schema must include guidelines for granting or denying particular types of accesses to the application system/database and should be included as part of an application system’s security plan. The program manager must obtain clearance on the protection schema from IRM/OPS/ITI/SI before implementation of the schema. The program manager is responsible for ensuring that the protection schema is enforced by the ISSO.

j. Upon major or minor modifications to a Department sponsored mainframe AIS application system or database, the program manager will review the protection schema that is in place for the application system/database and make revisions where necessary. The program manager must obtain clearance from IRM/OPS/ITI/SI on such revisions before implementation. The program manager is responsible for informing the ISSO of any revision to the protection schema.

k. The ISSO must implement access controls to the mainframe AIS application or database according to the guidance and instructions of the program manager. In the absence of explicit instructions governing any particular instance of requested access, the ISSO must obtain the approval of the applicable program manager prior to granting access.

l. Applications residing on classified mainframe AISs, including applications interacting with classified mainframe AISs from other systems, must be certified secure by DS/CIS/IST and IRM/OPS/ITI/SI before they are released to the field. (This certification will assure that these applications meet national standards for applications security.)

m. Annually, DS will report to the Undersecretary for Management the extent to which the Department's classified mainframe AIS applications, including applications interacting with classified mainframes from other systems, have been certified secure.

12 FAM 633.2 Security Controls

12 FAM 633.2-1 Access Controls

(TL:DS-83; 10-07-2002)

a. The data center manager and the system manager must ensure that all security software provided is installed on the AIS. In addition, on mainframe AISs, the ISSO and the data center manager must obtain clearance from IRM/OPS/ITI/SI before installing or upgrading security software.

b. The data center manager and the system manager must ensure that a valid and appropriate logon procedure is assigned that controls processing options available to each AIS user. See 12 FAM 637 for additional information.

12 FAM 633.2-2 Workstations and Printers

(TL:DS-83; 10-07-2002)

a. When processing classified data, users must treat video display screens in the same manner as classified material.

b. The data center manager and the system manager must ensure that security screens are installed on all monitors of PCs and classified terminals. See 12 FAM 637 for additional information.

c. The data center manager and the system manager must logically restrict users to workstations and printers on an individual basis.

d. The data center manager and the system manager must ensure that the AIS automatically disconnects a logged-on workstation or terminal from the system or deactivates the keyboard after a predetermined period of inactivity.

e. The data center manager and the system manager must limit unsuccessful logon attempts from any workstation. See 12 FAM 637 for additional information.

12 FAM 633.2-3 Storage of Audit Trails

(TL:DS-69; 06-22-2000)

The data center manager and the system manager must store the audit trail in a file with the most stringent access restrictions available.

12 FAM 634 INFORMATION SYSTEM FACILITY SECURITY

12 FAM 634.1 Physical Security

(TL:DS-83; 10-07-2002)

a. Domestically, all AIS equipment used to process classified information must be located within a facility authorized to store and process classified information. Abroad, all AIS components must be located within a controlled access area (CAA). Physical security policy and standards in 12 FAM 500 must be implemented.

b. When unattended, all areas housing classified AIS equipment must be technically and physically secured with DS-approved locks and alarms. The following additional physical security requirements pertain to classified AIS equipment abroad.

c. Abroad, a classified AIS may only be installed after a pre-installation survey has been conducted for any area which will house classified AIS equipment. The RSO, the security engineering officer (SEO), or a representative from the engineering services center (ESC), and the IPO or a member of the regional information management center (RIMC) normally perform these surveys.

d. For posts with 24-hour cleared U.S. citizen guards, all areas housing classified AIS equipment must be equipped with intrusion detection systems.

e. For posts without 24-hour cleared U.S. citizen guards, classified AIS equipment must be stored in a vault or secure room and a supplemental entry verification system (SEVS) must be installed. See 12 FAH-6, *OSPB Security Standards and Policy Handbook*, for SEVS requirements.

f. If a SEVS activates in a location where classified processing is performed, post must notify DS/IST/ISP and DS/IST/STO, and await further instruction prior to using any classified AIS equipment housed in the affected area.

g. The data center manager and the system manager must ensure that all major components of a distributed classified AIS are located within the information programs center. See 12 FAM 637 for additional information.

h. The data center manager and the system manager must ensure that there is no interconnectivity with an unclassified AIS.

12 FAM 634.2 TEMPEST Separation

(TL:DS-69; 06-22-2000)

TEMPEST separation and zone-of-control requirements will be determined on a case-by-case basis by the Department's certified TEMPEST Technical Authority (CTTA).

12 FAM 635 MICROCOMPUTER SECURITY

12 FAM 635.1 Physical Security: Access Control and Media Protection

(TL:DS-83; 10-07-2002)

a. Personnel accessing multi-user PCs should store all information on floppy diskettes. If all users accessing the PC have a valid need to share information, users may store information on the removable hard disk drive so that data is accessible to other personnel. See 12 FAM 637 for additional information.

b. The system manager must equip all standalone microcomputers with security enhancement controls as identified by the Department such as software products, host-dependent firmware products, independent

processor hardware products, etc.

c. The system manager and ISSO ensure that all classified microcomputers use completely removable magnetic media (floppy diskettes and hard disk packs). The magnetic media must be stored in a security container approved by DS for the storage of classified information. The container must be secured when unattended.

d. Abroad, the system manager must ensure that a PC and its associated printer use power from the same electrical outlet or a multiple outlet strip to ensure that grounds will be at the same potential.

12 FAM 635.2 Administrative Security: Authorized Use of Microcomputers

(TL:DS-69; 06-22-2000)

a. System users must ensure that classified U.S. Government information is not processed on privately owned microcomputers.

b. The installation of U.S. Government software on privately owned microcomputers is prohibited when in violation of host-country law, international copyright law, and/or a licensing agreement. A U.S. citizen direct-hire supervisor must approve in advance each installation of U.S. Government-owned software on a privately owned microcomputer, as being for the performance of official business. Media used to install U.S. Government software on a privately owned microcomputer may not subsequently be installed on a U.S. Government computer.

c. Media, e.g., diskettes that have been approved to transfer information from a privately owned microcomputer to a U.S. Government system must be checked for viruses on a standalone U.S. Government microcomputer immediately before the transfer.

12 FAM 636 CLASSIFIED AUTOMATED INFORMATION SYSTEMS PROCESSING AT CRITICAL TECHNICAL THREAT POSTS

(TL:DS-83; 10-07-2002)

a. The following additional system requirements apply to critical technical threat posts. All AISs processing classified *information* at critical technical threat posts must adhere to the following rules.

b. The data center manager, system manager and ISSO must ensure that equipment used to process classified information was certified by IRM/OPS, shipped to post via classified pouch, and stored at post

according to DS requirements.

c. The data center manager and the system manager must ensure that classified information is processed within a certified shielded enclosure (CSE) with a fingerstock door located within a parent room which meets Department shielding standards. The parent room must be locked and alarmed when unattended.

d. The data center manager and the system manager must ensure that only IRM/OPS-approved TEMPEST-certified laser printers are used for the production of hard copy output.

e. The security engineering officer (SEO) must ensure that all power for the classified AIS is provided via a motor generator set.

f. The data center manager, system manager and ISSO must make certain that classified AIS equipment is maintained only by IRM/OPS authorized personnel.

g. For posts without 24-hour cleared U.S. citizen guards, classified AIS equipment must be stored in a vault and a supplemental entry verification system (SEVS) must be installed. See 12 FAH-6*, OSPB Security Standards and Policy Handbook*, for SEVS requirements.

h. The data center manager and the system manager may not permit red signaling connectivity to AISs, including communications systems, located outside of a certified shielded enclosure (CSE).

i. The data center manager, system manager and ISSO must return damaged or unusable hard disk packs to IRM/OPS for destruction.

12 FAM 637 GENERAL PROCEDURES

12 FAM 637.1 Administrative Security

12 FAM 637.1-1 Shipping and Installation

(TL:DS-69; 06-22-2000)

a. AISs used for classified processing may only be installed at posts authorized for storage of classified information. The highest level of processing authorized is commensurate with the highest level of storage authorized but shall not exceed Secret.

b. The data center manager and the system manager must ensure that only classified AIS equipment which has been shipped to post via classified pouch and continuously maintained in controlled access areas (CAAs) is used to process classified information.

12 FAM 637.1-2 Password Controls

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager must retain copies of all password receipts for audit purposes at least six months after termination of the password, with the exception of password receipts/security acknowledgements, which shall be kept for the duration of the user's access to that AIS and for six months after the user's departure.

b. The data center manager and the system manager must delete from the AIS all user IDs and passwords supplied by the vendor for use during system manufacture and after each software installation. Default user IDs and passwords, such as "CSG," "System," "Field," "Test," must be removed from the AIS.

12 FAM 637.1-3 Use of Systems

(TL:DS-69; 06-22-2000)

a. The ISSO is authorized to allow supervisors access to subordinates' files.

b. Users who leave classified workstations logged on when unattended are subject to security violations outlined in 12 FAM 500.

c. The cabinet cover for classified impact printers must be closed and secured when operating.

d. Users must process NODIS and EXDIS information under the most stringent access controls available on the AIS. NODIS and EXDIS information should remain on the AIS only a minimal amount of time. Users must inform the data center manager and the system manager when NODIS and EXDIS information is placed on the AIS. The data center manager and the system manager must delete or archive NODIS and EXDIS information from the AIS as soon as it is no longer needed.

12 FAM 637.1-4 Protection of Media and Output

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager instruct users to protect all media used on and all hard copy material generated by classified AISs according to 12 FAM 500, which defines requirements for marking, classifying and declassifying, accountability, transportation, transmission, storage, and destruction of national security information.

b. Media normally controlled by general users (i.e., TEMPEST personal computer [TPC] removable disk packs, diskettes) must be

appropriately stored in a container approved for the storage of classified information. The container must be secured when unattended.

c. Media which has been used on an unclassified mainframe or nonmainframe AIS may not be loaded onto an AIS approved for classified processing unless specifically authorized by DS/CIS/IST.

12 FAM 637.1-5 Violations and Infractions

(TL:DS-69; 06-22-2000)

Individuals who do not comply with AIS policies and procedures will be subject to the violations and infractions regulations established by DS/ISP/APB and contained in 12 FAM 500. These regulations outline procedures for:

(1) Reporting and recording violations;

(2) Types of infractions for which violations can be issued; and

(3) Disciplinary action which may be imposed for security violations.

12 FAM 637.1-6 Disposition of Media, Output, and Equipment

(TL:DS-69; 06-22-2000)

a. Media must be sent via classified pouch. Classified media belonging to tenant agencies is also handled by the Digital Maintenance Branch in accordance with established MOUs. If disassembly tools are not available, Winchester and hermetically sealed packs may be shipped intact. Packages must be marked "For Disposition" and carry the appropriate classification. Approved degaussers for sanitizing media may be obtained from IRM/OPS.

b. Proper instructions for the disposal of classified laser toner cartridges are outlined in 12 FAM 500.

12 FAM 637.1-7 System Maintenance

(TL:DS-69; 06-22-2000)

The RSO must determine that all maintenance personnel with access to post AISs possess Top Secret clearances. The RSO should maintain a log which should include the date of service, service performed, identification numbers of the software or hardware, personnel performing service, equipment removed or replaced, and system condition or status following service. Records must be retained for six months after the date of entry.

12 FAM 637.1-8 Security Reviews and Reports

(TL:DS-69; 06-22-2000)

a. A security review includes personnel, administrative, system, and physical security practices. DS/CIS/IST will provide post instructions which outline required report contents.

b. DS/CIS/IST will conduct periodic security evaluations of classified mainframe and nonmainframe AISs at posts. These evaluations consider the threat environment and address post implementation of applicable Federal and Department AIS security policies, procedures, and requirements.

c. IRM/OPS/ITI/SI will conduct ongoing monitoring and technical auditing of security controls on Department classified mainframe AISs.

d. The Mainframe Security Program manager must ensure that an annual independent audit is performed on the security controls of all mainframe AISs under his or her authority. A copy of the audit findings should be sent to IRM/OPS/ITI/SI.

12 FAM 637.1-9 Review of Audit Logs

(TL:DS-69; 06-22-2000)

a. The ISSO will review monthly audit reports for potential security-related incidents such as:

(1) Multiple logon failures;

(2) Logons at unusual times;

(3) Failed attempts to execute programs or access files;

(4) Addition, deletion, or modification of user or program access privileges; or

(5) Changes in file access restrictions.

b. The ISSO will securely store all audit reports for six months from the date of the last entry.

12 FAM 637.2 Log and Record Keeping System Operation

(TL:DS-69; 06-22-2000)

The data center manager and the system manager ensures that a system operations log is maintained for all classified AISs. The log must

contain a record of all normal daily operations, system power-up and power-down, media mounted and dismounted, backup and recovery operations, and general environmental conditions. Installation, removal, or modification of system or application software must be noted in the log. Any unusual events or operating conditions must also be documented. Logs will be maintained for a minimum of six months from the date of the last entry or until the equipment is removed.

12 FAM 637.3 Security Controls

12 FAM 637.3-1 Access Controls

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager must implement file, program, and data controls to limit access to users or groups of users with the same need to know. Need to know may be based on functional responsibilities, operational requirements, supervisory responsibilities, or on a combination of these factors.

b. On nonmainframe AISs, the system manager grants access privileges in three user categories: system security administrators, system staff, and general users. The access privileges for each category are as follows:

(1) System security administrators (SSAs) have full access to all system functions and all data on the AIS. They are the only users able to modify files containing individual system authentication data. The ISSO must assign SSA privileges to the minimum number of personnel required for effective management of the AIS;

(2) System staff members have access to system devices, programs, and resources; however, this level of access does not permit modification of security parameters or changes to system files containing user authentication data. The ISSO must limit operator privileges, granting them only to members of the system staff who require these privileges to perform their system administration responsibilities; and

(3) General users have access to applications and data files based on supervisor-defined user profiles. This level of system access does not permit operator and system administrator functions.

c. On mainframe AISs, the ISSO grants access privileges in five user categories: system security administrators, system staff, operations staff, programming staff and general users. The access privileges for each category are as follows:

(1) System security administrators (SSAs), including the ISSO, have

full access to all system security functions and all security-related data on the AIS. They are the only users able to modify files containing individual system authentication data. SSA privileges must be assigned to the minimum number of personnel required for effective security management of the AIS;

(2) System staff members, including the system manager, have access to all operating system related devices, programs, and resources. They are the only users authorized to update any component of the operating system. However, they are not permitted access to modify security related data files or files containing user authentication data. System staff privileges must be granted only to members of the system staff who require them to perform their system administration duties;

(3) Computer operations staff (e.g., operators, schedulers and change control technicians) have limited access to operating system-related devices, programs, and resources. They control production workflow, allocate machine resources to tasks, monitor system and network performance and service peripheral devices. They are not permitted system security administrator privileges. Operator privileges must be granted only to members of the operations staff who require them to perform their duties;

(4) Programming staff have access to their application-specific programs, libraries, test data files, etc. This level does not permit computer operations, system staff or system security administrator privileges. Programming privileges must be granted only to members of the programming staff who require them to perform their duties; and

(5) General users have access to applications and data files based on program manager defined user profiles. This level of system access does not permit programming, computer operations, system staff or system security administrator privileges.

12 FAM 637.3-2 Workstations and Printers

(TL:DS-69; 06-22-2000)

a. Users cannot display classified information on a screen when unauthorized or uncleared individuals are, for any reason, physically positioned to view the screen. Monitors must face away from windows.

b. If the predetermined number of logon attempts is exceeded, the AIS will lock out the workstation. Only the system staff is authorized to reset a workstation after lockout.

12 FAM 637.3-3 Establishing Audit Trails and Logs

(TL:DS-83; 10-07-2002)

The data center manager and the system manager enables the audit trail feature on the operating system and installs any required security software to record security incidents listed in 12 FAM 637.1-9.

12 FAM 637.3-4 *Operating System and Application Software*

(TL:DS-83; 10-07-2002)

a. The IMO, who is responsible for the systems for which development software is being planned, is also responsible for ascertaining the citizenship of the person(s) working on this software project. If any person intending to be hired is a citizen of a country for which DS/DSS/ITA has assessed a Critical Technical and/or Human Intelligence threat level, that person shall not be hired for the purpose of developing, modifying, or performing maintenance on software specifically developed for use on Department of State computer systems, unless authorization has been received from the Analysis and Certification Division of the Office of Information Security Technology (DS/CIS/IST/ACD). The responsible person must contact DS/CIS/IST/ACD to obtain approval before the work is begun.

b. The IMO should submit the following information to DS/CIS/IST/ACD:

(1) Name(s) of the individual(s) being considered for performance of the work;

(2) Name of company/vendor;

(3) Country of citizenship of each applicable individual;

(4) Name and brief description of the software;

(5) Purpose of the software, if new; purpose of the maintenance or modification of existing software;

(6) Identification of the destination system (e.g., OpenNet, Classnet, a standalone PC), and whether inside or outside of a Controlled Access Area;

(7) Program language to be used; and

(8) Sensitivity of the data on the destination system.

c. DS/CIS/IST/ACD, in coordination with other DS elements, will conduct an analysis of this information, and prepare a recommendation to allow or not allow the proposed work to commence. All recommendations will be forwarded to the Deputy Assistant Secretary for Countermeasures and Information Security (DS/CIS) for final determination.

12 FAM 637.4 Information System Facility Security

12 FAM 637.4-1 Physical Security Standards

(TL:DS-69; 06-22-2000)

Abroad, the data center manager and the system manager must ensure that all major components of a distributed classified AIS are located within the information program center. This includes the central processing unit of a classified information handling system, C-LAN file server, and mass storage devices.

12 FAM 637.4-2 Environmental Protection

(TL:DS-69; 06-22-2000)

a. The general services officer (GSO) must ensure that fire detection systems and alarms in information processing facilities are fully functional at all times.

b. The GSO must ensure that the fire suppression system meets the requirements established by A/FBO/FIRE.

12 FAM 637.4-3 Microcomputers

(TL:DS-69; 06-22-2000)

Users should periodically back up information stored on the hard drive, as this data is vulnerable to loss.

12 FAM 637.5 Classified Automated Information Systems Processing at Critical Technical Threat Posts

(TL:DS-69; 06-22-2000)

The data center manager and the system manager must ensure that proper zone of control requirements are maintained around a CSE.

12 FAM 638 AND 639 UNASSIGNED