CHAPTER 2, PART I
PHYSICAL SECURITY STANDARDS FOR INFORMATION TECHNOLOGY (IT) RESTRICTED SPACE

1 BACKGROUND

The United States Department of Agriculture houses and processes information relating to the privacy of US citizens, payroll and financial transactions, proprietary information and life/mission critical data. It is essential that this information be protected from the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction. USDA must protect information resources through layered physical security, high logical data security and effective security procedures and administration. Successful IT security protection dictates the physical control of restricted space that contains major USDA computer and telecommunications resources. The purpose of this chapter is to define the physical security standards for all IT equipment/devices in this space.

Many USDA facilities house highly sensitive critical IT infrastructure components. As such, it is essential that every precaution be used to safeguard this information capability. Information technology infrastructures will be housed in IT Restricted Space that meets the requirements of the physical security standards outlined below.

2 POLICY

All USDA agencies are responsible for coordinating the physical security requirements of their critical infrastructure resources. Specifically, agencies are responsible for coordinating the physical security requirements of all IT Restricted Space that includes Computer Facilities, Telecommunications/Local Area Network (LAN) Rooms, Web Farms, SCIFs and Isolation Zones. These standards apply to existing and planned space to be utilized for this purpose. While every IT facility may not meet the physical security standards outlined above, CS will work with the agency, functional business owner and others to develop acceptable short and long term mitigation strategies to meet the needs of the Department. IT Restricted Space will be controlled directly by USDA personnel who will have the ultimate responsibility for control of these areas. All IT Restricted Space will have a facility based Occupant

Emergency Plan. New or planned specifications for IT Restricted Space will contain a provision that the physical security requirements will be coordinated with Cyber Security far enough in advance during the design phase to ensure compliance with this policy. Pending revisions to the Federal Acquisition Regulations (FAR) to include security requirements, all agencies will include physical security requirements in all Statements of Work (SOW) and Procurement Requests for IT Restricted Space.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with a updated timeline for completion. CS will monitor all approved exceptions.

3 PROCEDURES

The Critical Infrastructure consists of those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation’s critical infrastructures have been physically and logically separate systems that have little interdependence. This is also true in the case of USDA’s Critical Infrastructure, which is managed collectively under different programs in the department. The goals of these programs are diverse and not always overlapping in their security efforts. USDA buildings that house Computing Facilities, Telecommunications/LAN Rooms, Web Farms, SCIFs and Isolation Zones equipment automatically are considered critical IT Infrastructure Restricted Space and USDA must provide a level of physical security commensurate with that designation. Devices, in these facilities, which process or access sensitive data on a recurring basis will be protected in accordance with minimum security protection standards. IT Restricted Space areas must be secured in accordance with the requirements specified below:

a General Facility Security Requirements

Physical security for this space will be provided in compliance with the recommendations established for Federal Facilities by the Department of Justice, Vulnerability Assessment, dated June 28, 1995.

(1) Parking: Facility parking will be controlled; signs will be posted and arrangements will be made for towing of unauthorized vehicles; adequate lighting will be provided for parking areas;

(2) Closed Circuit Television (CCTV): CCTV surveillance cameras with time-lapse video recording will be provided;

(3) Lighting: Lighting with emergency power backup will be provided;

(4) Access Control: Facility will be controlled by armed security guards and an intrusion detection system with central monitoring capability maintained to current life safety standards;

(5) Entrances/Exits: High security locks will be installed and used;

(6) Employee/Visitor Identification: Agency photo ID will be required for all personnel and ID will be displayed at all times; visitors will be controlled and screened;

(7) Utilities: Utility access will be restricted to authorized personnel; emergency power will be provided to all critical systems (alarms, radio communications, computer facilities, etc.);

(8) Occupant Emergency Plans (OEP): OEPs will be implemented in facilities, updated and tested annually;

(9) Training: Annual Security Awareness Training will be conducted.

b General IT Restrictions –

(1) Prior to the determination of a IT Restricted Space location, consideration will be given to its proximity to public areas. Public areas are defined as areas that are maintained for or can be used by the public or the general community, such as rest rooms, libraries or visitor centers. IT Restricted Space

should not be located either above, adjacent, or below public areas in multi-story buildings;

(2) All packages being delivered to the IT Restricted Space will be x-rayed first. All mail/packages must be recorded in a log book;

(3) Periodic inspections of the door locking mechanism will be conducted by agency IT personnel on a bi-annual basis to provide assurance that hardware cannot be easily manipulated to gain unauthorized access;

(4) The roving guard will periodically inspect IT Restricted Space entrances for signs of forced entry; and

(5) Signage indicating IT Restricted Space locations is prohibited.

c <u>Physical Security Standards for IT Restricted Space</u> -

(1) The IT Restricted Space will be located in the interior of the building away from exterior windows, if practical;

(2) If floor plans are used at entrances to identify locations within the facility, critical asset locations will not be identified;

(3) Wall construction of the IT Restricted Space will be slab-to-slab with Sound Transmission Class 40 or better and other criteria cited in the ISC Security Design Criteria for Federal Buildings;

(4) The computer room will be protected by a fire suppressant system in accordance with local fire code, preferably dry-pipe;

(5) Entrances to the IT Restricted Space will be kept to the minimum required by local fire code;

(6) Activities with visitor populations will be located a minimum of 50 feet from IT Restricted Space ;

(7) Mailrooms will not be located within 50 feet of IT Restricted Space and cannot be placed over or under this space;

(8) Storage areas and loading docks will not be located within 50 feet of IT Restricted Space and cannot be placed over or under this space;

(9) Glass doors or windows will not be used in IT Restricted Space;

(10) Metal clad doors or solid wood doors with a 2-hour fire rating will be used at all IT Restricted Space entrances;

(11) Entrance to the computer room will be via electronic access control with the capability of providing an audit trail; Biometric Systems are encouraged;

(12) Exterior computer room doors having key access hardware will be removed from the Master Key system of the facility;

(13) The issuance of non-Master Keys must be controlled only to individuals with an ongoing business need;

(14) An intrusion detection system will be installed on all computer room entrances;

(15) The access control and intrusion detection systems will have Uninterrupted Power Supply (UPS) backup;

(16) Exterior IT Restricted Space doors will have either interior hinges or exterior hinges with non-removable pins;

(17) Based on the determination of mission criticality by each agency, computer rooms and web farms will have back-up generators and UPS;

(18) Weapons are not allowed in IT Restricted space with the exception of armed security officers, law enforcement and other investigative personnel; and

19) Backup tapes that contain mission critical or sensitive information will be stored offsite.

d <u>Personnel Security Requirements</u> –

(1) Only personnel having an ongoing recurring business need will be given unescorted access to the IT Restricted Space;

(2) Personnel who no longer have a business need to enter Restricted Space will immediately be removed from the access control system;

(3) Visitors should be kept to a bare minimum; tours by non-USDA personnel are prohibited;

(4) A sign in/sign out logbook shall be required for all escorted visitors; as a minimum the logbook shall contain the printed identity of each visitor, visitor’s signature, agency/company represented, purpose of visit, date/time in and date/time out;

(5) Cleaning and maintenance personnel shall be escorted at all times by USDA or permanent contractor personnel;

(6) An individual who has knowledge of the system being worked on shall escort non-permanent contractors needing access to the IT Restricted Space at all times; and

(6) A quarterly access review by the agency will be conducted of designated personnel (i.e., maintenance) having an ongoing business need in all restricted space.

e Web Farm Restricted Requirements

(1) Web Farms located in rooms other than a secure computing facility will be subject to the same physical security requirements outlined above; sections a-d above apply; and

(2) The room must have Web Farm computing equipment contained in secured cabinets.

4 RESPONSIBILITIES

a The Chief Information Officer/Deputy will:

Promote and support effective physical security standards for all USDA Information Technology (IT) Restricted Space.

b The Associate CIO for Cyber Security will:

(1) Publish physical security standards for all USDA Information Technology (IT) Restricted Space, to include Computer Facilities, Web Farms, Telecommunications/Magnetic Media Rooms, SCIFs and Isolation Zones ;

(2) Actively participate in the planning and design of all new IT Restricted Space to ensure that IT physical security standards are incorporated in space layouts for offices, buildings and complexes;

(3) Conduct on-site reviews of all existing IT Restricted Space to ensure that all Mission Critical, Departmental Priority and Sensitive Systems are protected through adequate layered physical security;

(4) Provide subject matter expert advice to USDA agencies on physical security standards as they relate to IT Restricted Space; and

(5) Review all exception requests concerning compliance time limit extensions or alternate methods of mitigating physical security risks by USDA agencies as they relate to IT Restricted Space.

c <u>The Associate CIO for Information Resources Management (IRM) will:</u>

(1) Support exception requests from the policy and procedures contained in this chapter to ensure that appropriate security protection is provided to all USDA IT Restricted Space; and

(2) Receive, review and coordinate a response with the Associate CIO for Cyber Security.

d <u>The Agency Chief Information Officer will</u>:

(1) Ensure that all agency personnel, especially the Agency Information System Security Program Manager (ISSPM) are aware of the policy and procedures concerning Restricted IT Space;

(2) Proactively consult with the Associate CIO for Cyber Security when planning or designing IT space in new buildings or space for the Information Technology (IT) infrastructure in an existing facility;

(3) Ensure that reviews are conducted of all agency IT Restricted space to make certain that they comply with the physical security requirements of this manual within <u>120 days</u> from issuance of this manual. Facilities that contain mission critical, departmental priority or sensitive systems will be reviewed by OCIO at least annually for compliance with physical security requirements;

(4) Provide a written report of all IT Restricted Space facilities not in compliance with these requirements to the Associate CIO for Cyber Security within <u>150 days</u> from issuance of this document;

(5) Send a written exception request for additional compliance time signed by the Agency Chief Information Officer with an Action Plan to mitigate standards not in compliance, milestones to accomplish mitigation efforts and timeframes

for completion or an action plan and timeframe to achieve compliance with all the physical security requirements in this document; and

(6) Include these requirements in all Statements of Work (SOW) and Procurement Requests for IT Restricted Space until there is a permanent revision of the FAR.

e Agency Managers for IT Restricted Space that includes Computer Facilities, Web Farms, Sensitive Compartmented Information Facilities (SCIF) and Isolation Zones will:

(1) Ensure that facilities under their control comply with all physical security requirements outlined in this manual;

(2) Collaborate with agency CIO and ISSPM for each location/facility that does not meet these requirements to prepare a exception request package; this request will include an Action Plan to mitigate standards not in compliance, milestones to accomplish mitigation efforts and timeframes for completion or an action plan and timeframe to achieve compliance with the physical security requirements in this document;

(3) In coordination with the agency ISSPM, perform regular annual reviews of all IT Restricted Space under their jurisdiction to ensure compliance with these requirements; and

(4) Facilitate the planning and design of all new IT Restricted Space to ensure that plans include the physical security standards outlined in this chapter.

f The agency Information System Security Program Managers/staff will:

(1) Coordinate the planning and design of all new IT Restricted Space to ensure that the space meets the physical security standards outlined in this chapter;

(2) Lead agency reviews of IT Restricted Space on a regular basis to ensure that they continue to comply with standards outlined in this directive; and

(3) Identify non-compliant IT Restricted Space locations, note areas of deficiencies, identify mitigations necessary. In coordination with the agency facility manager, prepare the exception request package for the Office of Cyber Security to meet the timeframes outlined above.

-END-