

DOCUMENTS, LAWS, RULES, REGULATIONS, & OTHER DATA

Office of Security Services: Physical Security Division

- **Code of Federal Regulations**
 - 7 CFR Part 331 and 9 CFR Part 121, Agricultural Bioterrorism Protection Act of 2002; Possession, Use, and Transfer of Biological Agents and Toxins; Final Rule
 - Establish and enforce safety procedures for listed agents and toxins, including measures to ensure proper training and appropriate skills to handle agents and toxins, and proper laboratory facilities to contain and dispose of agents and toxins;
 - Establish and enforce safeguard and security measures to prevent access to listed agents and toxins for use in domestic or international terrorism or for any other criminal purpose;
 - Establish procedures to protect animal and plant health, and animal and plant products, in the event of a transfer or potential transfer of a listed agent or toxin in violation of the safety procedures and safeguard and security measures established by the Secretary;
 - Ensure appropriate availability of biological agents and toxins for research, education, and other legitimate purposes.
- **ACTS:**
 - Anti-Terrorism Act 2002.
 - To combat terrorism and defend the Nation against terrorist acts, and for other purposes.
 - Critical Infrastructure Information Act – Information Analysis and Infrastructure Protection.

- The Critical Infrastructure Information Act of 2002 (CII Act) seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the nation's vulnerability to terrorism.
- USA PATRIOT Act of 2001 (42 U.S.C. 5195c (e))
 - The Act increases the ability of law enforcement agencies to search telephone, e-mail communications, medical, financial, and other records; eases restrictions on foreign intelligence gathering within the United States; expands the Secretary of Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and enhances the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts. The act also expands the definition of terrorism to include domestic terrorism, thus enlarging the number of activities to which the USA PATRIOT Act's expanded law enforcement powers can be applied.
- Homeland Security Act of 2002 (6 U.S.C. 101(9))
 - Establishment. - "There is established a Department of Homeland Security, as an executive department of the United States within the meaning of title 5, United States Code.
 - In General. - The primary mission of the Department (DHS) is to
 - prevent terrorist attacks within the United States;
 - reduce the vulnerability of the United States to terrorism; and
 - Minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States."

- Federal Information Security Management Act of 2002:
 - To promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act including:
 - Standards for categorizing information and information systems by mission impact
 - Standards for minimum security requirements for information and information systems
 - Guidance for selecting appropriate security controls for information systems
 - Guidance for assessing security controls in information systems and determining security control effectiveness
 - Guidance for certifying and accrediting information systems.
- Chemical Facility Anti-Terrorism Act of 2008:
 - The Department of Homeland Security has issued Chemical Facility Anti-Terrorism Standards for any facility that manufactures, uses, stores, or distributes certain chemicals at or above a specified quantity.
- Privacy Act (5 U.S.C. 552a)
 - The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to –
 - permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;
 - permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from

being used or made available for another purpose without his consent;

- permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;
- collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;
- permit exemptions from such requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and
- be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

- **Homeland Security Presidential Directives:**

- HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection:
 - This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.
- HSPD-8: National Preparedness:
 - This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national

domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.

- HSPD-9: Defense of United States Agriculture and Food:
 - This directive establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.
- HSPD-12: Common Identification Standard for Federal Employees and Contractors. (NIST FIPS 201-1, 800 Series, and OMB Directives):
 - There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.
- HSPD-20: National Continuity Policy:
 - This directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies. This policy establishes "National Essential Functions," prescribes continuity requirements for all executive departments and agencies, and provides guidance for State, local, territorial, and tribal governments, and private sector organizations in order

to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

- **Departmental Regulations/Manuals/Handbooks:**

- Integrated Physical Security Standards and Procedures (IPSSP).
 - Physical Security Divisions Integrated Physical Security Standards and Procedures that outline and define the following Security practices:
 - Physical Security
 - Aviation Security
 - Cyber Computer Security
 - Chemical, Biological, and Radiological Security
 - Personnel Security
 - Self Assessment
- Departmental Manual DM4620-002: Common Identification Standard for U.S. Department of Agriculture Employees and Contractors.
 - This Departmental Manual (DM) provides policies and procedures for USDA staff to meet the Personal Identity Verification (PIV) requirements of the directives and standards:
 - Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
 - U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Federal Information Processing Standard Publication 201-1 (FIPS 201-1),

Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006

- Office of Management and Budget (OMB) Memorandum, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors M-05-24, August 5, 2005
- OMB Memorandum, Acquisition of Products and Services for Implementation of HSPD-12, M-06-18, June 30, 2006
- Office of Personnel Management (OPM) Memorandum, Interim Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12, December 18, 2007 U.S. Department of Commerce, National Institute of Standards and Technology, Special Publications (SP):
 - 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004
 - 800-53, Recommended Security Controls for Federal Information Systems, February 2005
 - 800-63, Electronic Authentication Guideline, Appendix A, June 2004
 - 800-73-1, Interfaces for Personal Identity Verification, April 2006
 - 800-76-1, Biometric Data Specification for Personal Identity Verification, January 2007
 - 800-78-1, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, July 2006

- 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, July 2005
- 800-85a, PIV Card Application and Middleware Interface Test (SP 800-73 Compliance), April 5, 2006
- 800-85b, PIV Data Model Conformance Test Guidelines, July 2006
- 800-87, Codes for the Identification of Federal and Federally Assisted Organizations, January 2006.
- 800-96, PIV Card/Reader Interoperability Guidelines, September 2006
- 800-104, A Scheme for PIV Visual Card Topography
- Federal Acquisition Regulation, FAR Case 2005-15, Common Identification Standard for Contractors
- Office of Personnel Management (OPM) Memorandum, Interim Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12, December 18, 2007
- Departmental Regulation DR4620-002: Common Standard for U.S. Department of Agriculture Employees and Contractors.
 - This regulation prescribes the policies, roles, and responsibilities necessary to implement Homeland Security Presidential Directive (HSPD) 12, Common Identification Standard for Federal Employees and Contractors.
- **Interagency Security Committee (ISC):**
 - ISC Primary Member:
 - The Interagency Security Committee's standards, policies and best practices serve the needs of physical security managers

who are responsible for protecting nonmilitary federal facilities. These documents provide the federal community with strategies for physical security policies and standards that govern federal facilities protection. These strategies and standards facilitate the implementation of security policies and ensure a smooth implementation of mandatory standards.

- The Interagency Security Committee partners with other security organization to promote standards, standardize and apply uniform requirements, share information and collaborate, and advance best practices.
- Facility Security Level Determination for Federal Facilities:
 - Facility Security Level Determinations for Federal Facilities—An Interagency Security Committee Standard” (the Standard) defines the criteria and process to be used in determining the facility security level (FSL) of a Federal facility, a categorization which then serves as the basis for implementing protective measures under other ISC standards.
- Best Practices for Safe Mail Handling:
 - This document was developed by the ISC Safe Mail Handling sub-committee and identifies best mail room operations practices used by federal agencies. This unclassified document is provided to assist security managers in implementing safe mail handling practices at their facilities.
- Physical Security Criteria for Federal Facilities:
 - Physical Security Criteria for Federal Facilities—An Interagency Security Committee Standard” (the Standard) establishes a baseline set of physical security measures to be applied to all Federal facilities at each FSL – I, II, III, IV, and V. Further, the Standard provides a framework for the customization of security measures to address unique risks faced at each facility.

- Chemical Facility Anti-Terrorism Standard (CFATS)
 - Chemicals of Interests List (Appendix A)
 - The U.S. Department of Homeland Security has released an interim final rule that imposes comprehensive federal security regulations for high-risk chemical facilities.
 - This rule establishes risk-based performance standards for the security of our nation's chemical facilities. It requires covered chemical facilities to It requires covered chemical facilities to prepare Security Vulnerability Assessments, which identify facility security vulnerabilities, and to develop and implement Site Security Plans, which include measures that satisfy the identified risk-based performance standards.
 - It also allows certain covered chemical facilities, in specified circumstances, to submit Alternate Security Programs in lieu of a Security Vulnerability Assessment, Site Security Plan, or both.
 - National Infrastructure Protection Plan (NIPP):
 - The National Infrastructure Protection Plan provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the nation's critical infrastructure and key resources (CIKR) into a single national program. The overarching goal of the NIPP is to build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our nation's CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.

- NIPP-SSP-AG-FOOD: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan
 - Triennial Rewrite and Reissue of the Sector-Specific Plans (SSP)
 - Each Sector-Specific Agency is responsible for developing and implementing a Sector-Specific Plan (SSP), which details the application of the NIPP framework to the unique characteristics and conditions of their sector.
 - The Sector-Specific Plans (SSPs) detail the application of the National Infrastructure Protection Plan (NIPP) risk management framework to the unique characteristics and risk landscape of each sector and provide the means by which the NIPP is implemented across all critical infrastructure and key resources (CIKR) sectors. Each Sector-Specific Agency developed an SSP through a coordinated effort involving their public and private sector CIKR partners.
- **Office Systems, & Methods:**
 - Enterprise Physical Access Control System (ePACS).
 - HSPD-12 requires that USDA use "Secure and reliable forms of identification" for purposes of this directive means identification can be rapidly authenticated electronically.
 - Additionally, HSPD-12 requires the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to federally controlled facilities.
 - Currently, USDA agencies have over 200 individual PACS from various manufacturers. To meet the requirement of HSPD-12, USDA has built an Enterprise Physical Access Control System (ePACS) to integrate all USDA agency PACS.
 - Geospatial Security Information System (GeoSIS)

- GeoSIS was designed to provide a view of all USDA facilities and security assessment data at the national, state, and capitol regions and facility levels.
- Features of GeoSIS include:
 - Stores assessment physical site data for USDA facilities (threats and vulnerabilities)
 - Provides geographical data layers to display facility geographical data (facility locations across the U.S.)
 - Provides analytical tools that may recommend countermeasures to address physical security vulnerabilities
 - Provides facility site information to aid in analysis and decision support (facility mission, personnel, and assets.)
- Critical Risk Information System (CRIS)
 - CRIS is a web-based self assessment tool that leads responders through completing a site summary risk assessment to identify potential risk areas.
 - Allows non security professionals to perform a short term valuable risk assessment to be followed-up by the guidance of a physical security professional.
 - CRIS is designed to facilitate field data collections through structure and ease-of-use
 - CRIS allows USDA to identify possible vulnerabilities and risks at over 25,000 facilities in a cost effective and timely manner.
- USDA Security Assessment Methodology :
 - Based on the Government Accountability Office (GAO) Risk Based Assessment Methodology.

- The approach is used to identify threats, vulnerabilities and consequences of the risks. This approach has been used successfully on over 400 USDA facilities including; Aircraft hangars, laboratories, high hazard dams, data centers, office buildings, and Secretary's residence.
- The methodology consists of:
 - Asset Identification
 - Criticality Analysis
 - Threat Analysis
 - Vulnerability Analysis
 - Risk Analysis
 - Gap Analysis
 - Countermeasure Recommendations
 - Mitigation
- DCID6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)
 - Physical security standards are hereby established governing the construction and protection of facilities for storing, processing, and discussing Sensitive Compartmented Information (SCI) which requires extraordinary security safeguards. Compliance with this DCID 6/9 Implementing Manual (hereafter referred to as the "Manual") is mandatory for all Sensitive Compartmented Information Facilities (SCIFs) established after the effective date of this manual, including those that make substantial renovations to existing SCIFs. Those SCIFs approved prior to the effective date of this Manual will not require modification to meet these standards.

- **Procurement:**

- Federal Acquisition Regulations (FAR):

- The FAR is the primary regulation for use by all Federal Executive agencies in their acquisition of supplies and services with appropriated funds. It became effective on April 1, 1984, and is issued within applicable laws under the joint authorities of the Administrator of General Services, the Secretary of Defense, and the Administrator for the National Aeronautics and Space Administration, under the broad policy guidelines of the Administrator, Office of Federal Procurement Policy, Office of Management and Budget.
- The FAR precludes agency acquisition regulations that unnecessarily repeat, paraphrase, or otherwise restate the FAR, limits agency acquisition regulations to those necessary to implement FAR policies and procedures within an agency, and provides for coordination, simplicity, and uniformity in the Federal acquisition process. It also provides for agency and public participation in developing the FAR and agency acquisition regulation.

- Agricultural Acquisition Regulations (AGAR):

- USDA activities have a variety of needs for which it is critical that vendors provide products of the highest quality and reliability. These products must be capable of being used with products already in USDA's inventory, and with products supplied by other vendors. Accordingly, qualification requirements may be defined for USDA Activities including systems of application, testing and record keeping, to assure that products, vendors, or manufacturers are tested and qualified prior to contract award. The imposition of a QR can restrict competition and as a result is strictly managed. If a QR does not appear on this listing, the requirement has not been approved by USDA and may neither be used nor enforced for USDA actions.

