DR 4620-xxx

United States
Department of
Agriculture

Office of Security Services

COMMON IDENTIFICATION STANDARD FOR U.S. DEPARTMENT OF AGRICULTURE EMPLOYEES AND CONTRACTORS

DR 4620-xxx

DRAFT

U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, DC 20250

DEPARTMENTAL REGULATION	**Number:** DR 4620-xxx
SUBJECT: Common Identification Standard for U.S. Department of Agriculture Employees and Contractors	**DATE: May 15, 2008**
	OPI: Office of Security Services (OSS)

DRAFT

Section		Page
1	Purpose	1
2	Background	1
3	Special Instructions/Cancellations	2
4	Policy	2
5	Credential Issuance	3
6	Roles and Responsibilities	3
Appendix A	Definitions	A-1
Appendix B	Acronyms	B-1
Appendix C	HSPD-12 Source Documents	C-1

1. PURPOSE

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 in the Department.

2. BACKGROUND

HSPD-12 establishes the general requirements for a common Federal identification system. The President has mandated that all Federal departments provide a process for identity proofing and credentialing employees and contractors to increase security and provide greater interoperability between departments and Federal facilities.

For further information on HSPD-12 and its related requirements and standards, please see sources in Appendix C.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

HSPD-12 applies to all Federal employees, as defined in title 5 U.S.C §2105 "Employee," within a department or agency. In addition, all contractors requiring unaccompanied access to federal facilities and/or federal information systems will be subject to HSPD-12 requirements.

No provision in this regulation shall have the effect of nullifying or limiting protections for equal employment opportunity as defined under Title VII of the Civil Rights Act, 42 U.S.C. 3535(d), or Executive Order 11478. USDA will not implement this regulation in such a way as to impede equal employment opportunity on the basis of race, color, religion, sex, national origin, age, or disability.

The 2002 Federal Information Security Management Act (FISMA) does not permit waivers to the Federal Information Processing Standard (FIPS) 201-1 standards.

This regulation cancels DR 4620-1 dated February 26, 1995.

4. POLICY

Departmental agencies must comply with HSPD-12 for all applicable USDA federal employees and contractors who work for USDA. Detailed procedures are described in Departmental Manual (DM) 4620-xxx.

a. Agencies must implement the standard procedures in FIPS 201-1, the NIST Special Publication (SP) series related to HSPD-12, and DM 4620-xxx.

b. All employees hired under Title 5 USC and Farm Services Agency (FSA) county employees will be required to follow procedures in FIPS 201-1, the NIST Special Publication (SP) series related to HSPD-12, and DM 4620-xxx, if they require unaccompanied access to USDA facilities and/or information systems.

c. All contractors working for USDA will be required to follow procedures in FIPS 201-1, the NIST Special Publication (SP) series related to HSPD-12, and DM 4620-xxx if they require unaccompanied access to USDA facilities and/or information systems.

d. All USDA employees who are stationed outside the United States at government facilities and/or have access to information systems will be issued credentials by the Department of State.

DRAFT

5. INITIAL CREDENTIAL ISSUANCE

Initial credentials will be issued in the following order: 1) those located in National Capital Region (NCR); 2) those located in USDA Mission Critical Facilities (MCF) and major metropolitan area facilities; and 3) all remaining field locations.

6. ROLES AND RESPONSIBILITIES

a. The Office of the Chief Information Officer (OCIO) will:

(1) Establish, in consultation with the Office of Security Services (OSS), policies, standards, and procedures for implementing and administering the PIV program throughout the Department.

(2) Ensure that the IT infrastructure is compatible with the GSA Shared Services Solution.

(3) Create requirements for the development of an enterprise Logical Access Control System (LACS), and build and maintain centralized LACS according to requirements.

(4) Assist OSS with maintaining an enterprise Physical Access Control System (ePACS) infrastructure and connectivity.

(5) Ensure personal information collected for employee and contractor identification purposes is handled consistent with the Privacy Act of 1974 (5 U.S.C. § 552a) and all FISMA requirements.

b. Departmental Administration – Office of Security Services (OSS) will:

(1) Establish, in consultation with the Office of the Chief Information Officer (OCIO), policies, standards, and procedures for implementing and administering the PIV program throughout the Department.

(2) Develop and implement policies and procedures to support the registration and identity proofing of contract employees, and to ensure initiation and adjudication of contract employee background checks (National Agency Check with Inquiries (NACI)).

(3) Assist agencies in determining if previous NACI, Public Trust or National Security Clearance background investigations were successfully adjudicated.

DRAFT

(4) Create requirements for the development of an ePACS to centrally support agency PACS; build and administer an ePACS according to requirements.

(5) Be responsible for the physical access control system for all USDA facilities within the NCR. Continue to support all facilities as previously required.

(6) Develop a master plan for initial implementation and credential issuance.

c. Departmental Administration – Office of Human Capital Management (OHCM) will:

(1) Develop policies and procedures to ensure that Agency Human Resources staff that in-process new employees capture the all information required for HSPD-12 enrollment,

(2) Develop policies and procedures to ensure a Background Investigation (NACI) has been initiated and successfully adjudicated.

(3) Determine the position sensitivity designation for all applicant positions, and ensure the employee has the appropriate background investigation commensurate with that determination.

(4) If an employee is denied a LincPass, he or she will be removed from Federal service. The appeal process for a removal from federal service is already established in law and regulation (Title 5, U.S.C. and Title 5, C.F.R.); employees can appeal to the Merit Systems Protection Board.

(5) Post to the public website a quarterly report on the number of PIV credentials issued to employees as required by OMB.

d. Departmental Administration – Office of Procurement and Property Management (OPPM) will:

(1) Provide HSPD-12 procurement and contracting guidance to the agencies and to the acquisition workforce.

(2) Support sponsorship training module development.

DRAFT

(3) Support OSS in development of roles and responsibilities for contractors.

(4) Review and distribute HSPD-12 relevant information to agency procurement operations as additional system requirements and operational procedures are defined by OPPM/PDSD and OCIO.

e. The Agencies will:

(1) Comply with NIST's FIPS 201-1, the NIST Special Publication series related to HSPD-12, and Departmental Manual 4620-xxx.

(2) Comply with Departmental policies and procedures to support registration, identity proofing, and issuing LincPasses and other appropriate badges.

(3) Prepare and validate data to be loaded into the GSA Shared Services system and provide roles for sponsorship, enrollment, adjudication, and activation for issuance of LincPasses.

(4) Ensure agency applicants' travel to enrollment stations for both enrollment and activation of their LincPasses.

(5) Ensure compatibility of agency physical and logical control systems with USDA enterprise physical and logical control systems; comply with USDA physical and logical control policies and procedures.

(6) In consultation with OPPM, provide HSPD-12 procurement and contracting guidance, to ensure compliance with HSPD-12, FIPS 201-1, and OMB guidance.

(7) Maintain records that will permit the audit of agency PIV programs in accordance with HSPD-12, FIPS 201-1, relevant OMB guidance and any OIG requirements.

f. GSA Shared Service Solution will:

(1) Provide USDA with a system to enroll, print, and activate LincPass smartcards to eligible individuals to meet HSPD-12 requirements.

- END -

DRAFT

APPENDIX A

DEFINITIONS

a. Access control. The process of granting or denying requests to access physical facilities or areas, or to logical systems (e.g., computer networks or software applications). See also "logical access control system" and "physical access control system."

b. Accompanied access. A person that is accessing the facility and/or information system under escort and/or continuous monitoring by a USDA official (PIV ID credential holder).

c. Contractor. An individual under contract to USDA (for the purpose of HSPD-12 implementation).

d. Credential. An identity card ("smart card") also known as LincPass issued to an individual that contains stored identity credentials so that the claimed identity of the cardholder can be verified against the stored credentials by another person or by an automated process.

e. Federal Facility or Information System Access. Authorization granted to an individual to physically enter federally controlled facilities, and/or electronically (logically) access federally controlled information systems for approved purposes.

f. Identity-proofing. The process of providing sufficient information (e.g., driver's license, proof of current address, etc.) to a registration authority, or the process of verifying an individual's information that he or she is that individual and no other.

g. LincPass. USDA has named their common ID card the LincPass, as it is designed to link a person's identity to an identification card and the card to a person's ability to access Federal buildings and computer systems. The spelling of LincPass is a tribute to President Abraham Lincoln, who created the People's Department (now USDA) in 1862.

h. Logical Access Control System (LACS). Protection mechanisms that limit a user's access to information and restrict their forms of access on the system to only what is appropriate for them. These systems may be built in to an operating system, application, or an added system.

i. Mission Critical Facility (MCF). A building or group of buildings in one geographical area, so vital to the United States and/or USDA that the incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, USDA mission accomplishment during exigent circumstances, or any combination thereof.

DRAFT

j. National Agency Check with Inquiries (NACI). The basic and minimum investigation required of all new Federal employees and contractors consisting of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the FBI Identification Division's name and fingerprint files, and other files or indices when necessary. A NACI also includes written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

k. National Capital Region (NCR). Pursuant to the National Capital Planning Act of 1952 (Title 40, U.S.C., Sec. 71) the Act defined the NCR as the District of Columbia; Montgomery and Prince George's Counties of Maryland; Arlington, Fairfax, Loudon, and Prince William Counties of Virginia; and all cities now or here after existing in Maryland or Virginia within the geographic area bounded by the outer boundaries of the combined area of said counties.

l. Physical Access Control System (PACS). Protection mechanisms that limit users' access to physical facilities or areas to only what is appropriate for them. These systems typically involve a combination of hardware and software (e.g., a card reader), and may involve human control (e.g., a security guard).

m. PIV-II Compliant Credential. An identity card ("smart card") also known as LincPass issued to an individual that contains stored identity credentials so that the claimed identity of the cardholder can be verified against the stored credentials by another person or by an automated process.

n. Unaccompanied access. A person that is accessing the facility and/or information system without an escort and/or continuous monitoring by a USDA official. The agency's determination should be based upon the support to successfully complete USDA's mission critical functions/missions. This type of access requires a mandatory PIV ID credential to be issued.

DRAFT

APPENDIX B

ABBREVIATIONS

DM	Departmental Manual
ePACS	Enterprise Physical Access Control System
FISMA	Federal Information Security Management Act
FIPS	Federal Information Processing Standard
FSA	Farm Services Agency
GSA	General Services Administration
GSA MSO	General Services Administration Managed Services Office
HSPD-12	Homeland Security Presidential Directive 12
LACS	Logical Access Control System
LincPass	PIV-II Compliant Badge for USDA
MCF	Mission Critical Facility
NACI	National Agency Check with Inquiries
NCR	National Capital Region
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPPM	Office of Procurement and Property Management
OSS	Office of Security Services
PACS	Physical Access Control System
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification, Part I
PIV-II	Personal Identity Verification, Part II
USDA	United States Department of Agriculture

DRAFT

APPENDIX C

HSPD-12 SOURCE DOCUMENTS

a. Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

b. Computer Security Act of 1987 (Public Law 100-235).

c. U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Federal Information Processing Standard Publication (FIPS) 201-1, Personal Identity Verification, March 2006

d. 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

e. OMB Memorandum, Acquisition of Products and Services for Implementation of HSPD-12, M-06-18, June 30, 2006

f. OMB Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials, M-07-06, January 11, 2007

g. Privacy Act, 1974 (5USC 552a) and Electronic Privacy Act, 1986 (USC 2701)

h. U.S. Department of Commerce, National Institute of Standards and Technology, Special Publications (SP):

(1) 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004
(2) 800-53, Recommended Security Controls for Federal Information Systems, September 2004 (2PD).
(3) 800-63, Electronic Authentication Guideline, Appendix A, June 2004.
(4) 800-73-1, Interfaces with Personal Identity Verification, April 2006.
(5) 800-76-1, Biometric Data Specification for Personal Identity Verification, January 2007.
(6) 800-78-1, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, July 2006.
(7) 800-85A, PIV Card Application and Middleware Interface Test Guidelines, April 2006.
(8) 800-87, Codes for the Identification of Federal and Federally-Assisted Organizations, December 2006.
(9) 800-104, A Scheme for PIV Visual Card Topology, January 2007.

i. Department Manual (DM 4620-xxx) Common Identification Standard for U.S. Department of Agriculture Employees and Contractors

DRAFT

j. Form I-9 (Rev. 10/4/00) – Department of Justice (OMB No. 1115-0136)

k. Personnel Investigations, Title 5, Code of Federal Regulations, 736.101 (b)

DRAFT