

**UNITED STATES DEPARTMENT OF AGRICULTURE
WASHINGTON, DC 20250**

DEPARTMENTAL REGULATION		Number: DR 4620-002
SUBJECT: Common Identification Standard for U.S. Department of Agriculture	DATE: September 29, 2014	
	OPI: Office of Homeland Security and Emergency Coordination (OHSEC)	

Section	Page
1 Purpose	1
2 Background	1
3 Special Instructions/Cancellations	2
4 Policy	3
5 Credential Issuance	3
6 Credential Utilization	3
7 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 and maintain Homeland Security Presidential Directive (HSPD) 12, Common Identification Standard for Federal, Non-Federal Employees and Contractors within USDA controlled work environments.

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

The issuance of the HSPD-12 credential, referred to now as the USDA LincPass, is mandatory and applies to all employees, as defined in [5 U.S.C §2105](#) (2014) “Employee,” within a department or agency. “Employee” means a person, other than the President and Vice President, employed by, detailed or assigned to, the U.S. Department of Agriculture (USDA), including members of the Armed Forces; an expert or consultant to USDA; an industrial or commercial contractor, licensee, certificate holder, or grantee of USDA, including all subcontractors; or any other category of person who acts on behalf of an agency as determined by the agency head. In addition, all contractors requiring routine access to federally controlled facilities and/or federally controlled 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 provided in [Title VII of the Civil Rights Act, 42 U.S.C. § 2000e, et seq.](#) (2014), and [Executive Order \(EO\) 11478](#). USDA prohibits discrimination in all its programs and activities on the basis of race, color, national origin, age, disability, and where applicable, sex, marital status, familial status, parental status, religion, sexual orientation, genetic information, political beliefs, reprisal, or because all or a part of an individual's income is derived from any public assistance program. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audiotape, etc.) should contact USDA's TARGET Center at (202) 720-2600 (voice and TDD). To file a complaint of discrimination write to USDA, Director, Office of Civil Rights, 1400 Independence Avenue, S.W., Washington, DC 20250-9410 or call 1-800-795-3272 (voice) or (202) 720-6382 (TDD). USDA is an equal opportunity provider and employer.

The only other authorized badge and credentials issued by USDA will be for law enforcement; investigations; food inspection; Plant, Protection and Quarantine; animal care; and physical security use. This authority will remain in the control of Agencies such as the Office of the Inspector General, the Forest Service, the Secretary's Personal Protection Team, the Food Safety & Inspection Service, the Animal Plant Health Inspection Service, the Office of Operations, and the Office of Homeland Security and Emergency Coordination.

This policy conforms with [Federal Information Security Management Act of 2002 \(FISMA\) 44 U.S.C. § 3541, et seq.](#) (2014) and [Federal Information Processing Standard \(FIPS\) 201-2](#) guidelines.

This regulation supersedes DR 4620-002 dated January 14, 2009.

4. POLICY

Enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, USDA-wide standard for secure and reliable forms of identification to its employees and contractors.

- a. Departmental agencies must comply with HSPD-12 for all applicable USDA federal and non-federal employees who work for USDA. Detailed procedures are described in [Departmental Manual \(DM\) 4620-002](#).
- b. Employees as defined by [5 U.S.C §2105](#) (2014), and non-federal employees working for USDA will be required to follow procedures in [FIPS 201-2](#), the NIST Special Publication (SP) series related to HSPD-12, and [DM 4620-002](#), if they require routine unaccompanied access to USDA controlled facilities and/or information systems.
- c. Employees who are stationed outside the United States at Government facilities may be issued a Department of State credential.

5. CREDENTIAL ISSUANCE

All applicable long term (more than one consecutive work year) employees, as described within this document, must be issued a LincPass as a condition of employment for unaccompanied access to IT and Facility infrastructure.

Short term personnel (less than one consecutive work year), such as student interns, volunteers, etc. could be issued an alternate credential as a condition of employment for limited unaccompanied access to IT and Facility infrastructure. See [DM 4620-002](#) for a list of alternate credentials.

For short-term personnel requiring unaccompanied access to necessary IT and Facility infrastructure, a LincPass must be issued.

6. CREDENTIAL UTILIZATION

For logical access requirements, see [DR 3170-001](#) (logical access requirements), [DR 3640-001](#) (ICAM), and [DM 4620-002](#) for further clarification.

For physical access requirements, see [DM 4620-002](#), Chapter #3 Physical Access Control Systems (PACS)

7. ROLES AND RESPONSIBILITIES

- a. The Chief Information Officer (CIO) will:
- (1) Maintain, in consultation with the Office of Homeland Security and Emergency Coordination (OHSEC), policies, standards, and procedures for implementing and administering the HSPD-12 program throughout the Department;
 - (2) Assist OHSEC with maintaining connectivity to the various enterprise systems that support HSPD-12 requirements; and
 - (3) Work with OHSEC to ensure personal information collected for employee and contractor identification purposes is handled consistent with the [Privacy Act of 1974 5 U.S.C. § 552a\(2014\)](#) and all FISMA requirements see [44 U.S.C. § 3541, et seq. \(2014\)](#).
- b. Director – Office of Homeland Security and Emergency Coordination (OHSEC) will:
- (1) Maintain, in consultation with the Office of the Chief Information Officer (OCIO), policies, standards, and procedures for implementing and administering the HSPD-12 program throughout the Department;
 - (2) Work with Agencies and Staff Offices to maintain policies and procedures to support the identity proofing, registration and credentialing of employees;
 - (3) Maintain an enterprise ePACS environment to support agency physical access control systems;
 - (4) Oversee and assist with migrating all physical access control systems into HSPD-12 compliance;
 - (5) Post to the public Web site a quarterly report on the number of LincPass credentials issued to employees as required by OMB;
 - (6) Support role holder training module development; and
 - (7) Support Agencies with the roles and responsibilities for managing non-federal employees including the establishment and implementation of the appeal and removal procedures for those denied a LincPass, in accordance with DM 4620-002.
- c. Director – Office of Human Resources Management (OHRM) will:
- (1) Develop, maintain, and disseminate on-boarding policies and procedures for agency Human Resources staff.

- d. Director – Office of Procurement and Property Management (OPPM) will:
 - (1) Provide HSPD-12 procurement and contracting guidance to the acquisition workforce through [Procurement Advisory 115](#); entitled Continued Implementation of LincPass at USDA;
 - (2) Preparation of guidance and BPAs to ensure that HSPD-12 compliant equipment is purchased.
- e. Chief Financial Officer (CFO) will:
 - (1) Maintain and update EmpowHR/Person Model in a timely manner; and
 - (2) Provide financial oversight and management of HSPD-12 funding.
- f. Agency Deputy Administrators of Management (DAMs) will:
 - (1) Comply with all relevant HSPD-12 requirements such as [NIST’s FIPS 201-2](#), NIST Special Publications, [DR 3170-001](#), [DR 3640-001](#), and [Departmental Manual 4620-002](#);
 - (2) Utilize the HSPD-12 risk assessment credential matrix for all federal and non-federal employees to determine eligibility for LincPass. To access the credential matrix see [DM 4620-002](#);
 - (3) Remove from Federal service any employee denied a LincPass. The appeal process for a removal from federal service is already established in law and regulation see [5, U.S.C. § 7513\(d\)](#) (2014); [5, C.F.R. § 752.405](#) (2014); employees can appeal to the Merit Systems Protection Board;
 - (4) Comply with Departmental policies and procedures to support registration, identity proofing, and issuing LincPasses and other appropriate badges;
 - (5) Ensure agency applicants’ complete enrollment and activation process for their LincPasses in a timely manner;
 - (6) Comply with USDA physical and logical control policies and procedures;
 - (7) In consultation with OPPM, ensure HSPD-12 products and services are compliant with [FIPS 201-2](#) and OMB guidance;
 - (8) Assign a point of contact and alternate to the HSPD-12 Program Office that can provide outreach to agency personnel;

- (9) Ensure HSPD-12 role holders are assigned, such roles as Sponsor, Security Officer, Adjudicator, Role Administrator, etc., to ensure employees receive their USDA credential in a timely manner; and
 - (10) Identify all personnel requiring Federal Emergency Response Official (FERO) designation and ensure that designation is on their LincPass credential by providing the list of names to the sponsor.
- g. The Employees will:
- (1) Comply with Departmental policies and procedures related to LincPass issuance and maintenance. This includes adhering to deadlines for credential and certificate renewal.

- END -

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. Access (Limited): A person that is accessing the facility and/ or information system, but only requires limited access. Limited access to facilities includes unaccompanied access to general common areas and workspace only. Limited access to information systems includes access to applications such as USDA email, Time & Attendance, AgLearn and GovTrip.
- c. Access (Accompanied). A person that is accessing the facility and/or information system under escort and/or continuous monitoring by a USDA official (LincPass credential holder).
- d. Access (Unaccompanied). 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 LincPass credential to be issued.
- e. Contractor. An individual under contract to USDA (for the purpose of HSPD-12 implementation).
- f. 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. There may be other approved forms of a credential when applicable.
- g. Employee. Defined in 5 U.S.C §2105 (2014) “Employee,” within a department or agency. “Employee” means a person, other than the President and Vice President, employed by, detailed or assigned to, USDA, including members of the Armed Forces; an expert or consultant to USDA; an industrial or commercial contractor, licensee, certificate holder, or grantee of USDA, including all subcontractors; or any other category of person who acts on behalf of an agency as determined by the agency head
- h. 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.

- i. Identity-proofing. The process of providing sufficient information (e.g., driver's license, proof of current address) to a registration authority, or the process of verifying an individual's information that he or she is that individual and no other.
- j. 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.
- k. 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.
- l. 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).
- m. 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).
- n. 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.
- o. Routine 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.

APPENDIX B

ABBREVIATIONS

DM	Departmental Manual
ePACS	Enterprise Physical Access Control System
FERO	Federal Emergency Response Official
FISMA	Federal Information Security Management Act
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
LACS	Logical Access Control System
LincPass	PIV-II Compliant Badge for USDA
NACI	National Agency Check with Inquiries
NIST	National Institutes of Standards and Technology
OCIO	Office of 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
OHSEC	Office of Homeland Security and Emergency Coordination
PACS	Physical Access Control System
USDA	United States Department of Agriculture

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, Pub. L. No. 100-235, 101 Stat. 1724 (1988), (codified as amended at scattered sections of 15 and 40 U.S.C.)
- 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. OMB M11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors, February 2011.
- h. Privacy Act of 1974, 5 U.S.C. § 552a (2014).
- i. U.S. Department of Commerce, National Institute of Standards and Technology, Special Publications (SP):
 - (1) 800-37-1, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
 - (2) 800-53-4, Security and Privacy Controls for Federal Information Systems and Organizations, February 2012.
 - (3) 800-63-1, Electronic Authentication Guideline, December 2011.
 - (4) 800-87-1, Codes for the Identification of Federal and Federally-Assisted Organizations, April 2008.
 - (5) 800-104, A Scheme for PIV Visual Card Topology, January 2007.
- j. Department Manual (DM 4620-002) Common Identification Standard for U.S. Department of Agriculture Employees and Contractors

- k. Department Regulation 3640-001 Identity, Credential, and Access Management
- l. Form I-9 (Rev. 10/4/00) – Department of Justice (OMB No. 1115-0136)
- m. 5, C. F.R. § 736.101
- n. 5 U.S.C §2105 (2014)
- o. 5 U.S.C. § 7513(d) 2014
- p. 5 C.F.R. § 752.405 (2014)
- q. Title VII of the Civil Rights Act, 42 U.S.C. § 2000e, et seq. (2014).
- r. Executive Order 11478, Equal Opportunity Employment in the Federal Government (1969).
- s. Federal Information Management Act of 2002 (FISMA), 44 U.S.C. § 3541, et seq. (2014).