DM 4620-002

United States
Department of
Agriculture

Office of Security Services

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

DM 4620-002

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

TABLE OF CONTENTS

U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, DC 20250

DEPARTMENTAL MANUAL	**Number:** DM 4620-002
SUBJECT: Common Identification Standard for U.S. Department of Agriculture Employees and Contractors	**DATE:** January 14, 2009
	OPI: Office of Security Services (OSS)

CHAPTER 1

OVERVIEW

1. PURPOSE

This Departmental Manual (DM) provides policies and procedures for USDA staff to meet the Personal Identity Verification (PIV) requirements of the directives and standards:

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

b. 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

c. 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

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

e. OMB Memorandum, Validating and Monitoring Agency Issuance of Personal Identity Verification Cards, M-07-06, January 11, 2007

f. 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, February 2005

(3) 800-63, Electronic Authentication Guideline, Appendix A, June 2004

(4) 800-73-1, Interfaces for 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) 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, July 2005

(8) 800-85a, PIV Card Application and Middleware Interface Test (SP 800-73 Compliance), April 5, 2006

(9) 800-85b, PIV Data Model Conformance Test Guidelines, July 2006

(10) 800-87, Codes for the Identification of Federal and Federally Assisted Organizations, January 2006.

(11) 800-96, PIV Card/Reader Interoperability Guidelines, September 2006

(12) 800-104, A Scheme for PIV Visual Card Topography

g. Federal Acquisition Regulation, FAR Case 2005-15, Common Identification Standard for Contractors

h. Office of Personnel Management (OPM) Memorandum, Interim Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12, December 18, 2007

HSPD-12 mandates the development and implementation of a mandatory, Government-wide Standard for secure and reliable forms of identification issued to Federal employees and contractors.

FIPS 201-1 (1) defines a reliable, Government-wide PIV system for use in applications such as access to Federally controlled facilities or information systems, (2) specifies a PIV system within which common identification badges can be

created and later used to verify a claimed identity, and (3) requires identity proofing and background investigations to verify identity.

OMB Implementation Memorandum M-05-24 provides guidance for implementing the requirements in FIPS 201-1 and HSPD-12. The guidance clarifies timelines, applicability, and the requirements of PIV-I and PIV-II. OMB Memorandum M-07-06 provides the guidance for reporting the number of PIV credentials issued by quarter. Beginning March 1, 2007 and each quarter thereafter, agencies will post their reports on their Federal agency public Web site.

USDA mission areas, agencies, and staff offices are referred to hereafter as "agency" or "agencies."

2. SPECIAL INSTRUCTIONS

DM 4620-002 is a new Departmental Manual and does not replace any previous Departmental Manual. Agency HSPD-12 designated Points of Contact (POC) are responsible for the distribution of DR 4620-002 and DM 4620-002 and the administration of the program within their agencies.

3. BACKGROUND

Government agencies use a wide range of methods to authenticate Federal employees and contractors as a requirement to enter Government buildings and use Government systems. Federal agencies use authentication mechanisms to allow access to specific areas or systems. The methods and level of assurance for authentication (i.e., identification) and authorization (i.e., permission) vary widely from agency to agency, and sometimes within a single agency.

HSPD-12 requires that all Government agencies develop specific and consistent standards for both physical and logical identification systems. NIST's FIPS 201-1 establishes detailed standards on implementing processes and systems to fulfill the requirements of HSPD-12. FIPS 201-1 outlines two phases to implementing an HSPD-12 program. Phase I (PIV-I) describes the registration and identity proofing process. Phase II (PIV-II) describes the technical and interoperability requirements of an HSPD-12-compliant system.

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

4. APPLICABILITY

According to FIPS 201-1, the standard "is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally- controlled facilities

and logical access to Federally-controlled information systems except for "national security systems" as defined by 44 U.S.C. 3542(b)(2).

Specifically, PIV applies to all Employees (as defined in title 5 U.S.C §2105 "Employee") within a department or agency. Further defined by Executive Order (EO) 12968, "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; a personal services contractor; or any other category of person who acts on behalf of an agency as determined by the agency head.

In addition, all part time employees and contractor employees who require routine access to federally controlled facilities and/or information systems will be subject to PIV. Federal employees who submitted their retirement paperwork and will retire within 6 months of submission are not subject to PIV and do not need to enroll in the HSPD-12 program. Refer to the LincPass Distribution Risk Assessment in Appendix D for guidance with regard to part time employees and contractors.

Temporary employees and contractors, short-term employees and contractors, guests, occasional visitors to Federal facilities, and individuals needing remote access to systems or applications can be issued alternate badges as described in Chapter 2, Section 6 of this Manual. These individuals are subject to a badge risk assessment just as full-time Federal employees and contractors are. Such individuals shall have in their written work agreements (volunteer agreement, guest researcher agreement, memorandum of understanding, extramural agreement, etc.) a statement as to whether the agency risk assessment requires a PIV ID credential, and the eligibility requirements for a PIV ID credential. Refer to the LincPass Distribution Risk Assessment in Appendix D and on the Physical Security website, http://www.usda.gov/da/pmd/physprop.htm.

FIPS 201-1 also contains a special-risk security provision: "The U.S. Government has personnel, facilities, and other assets deployed and operating worldwide under a vast range of threats (e.g., terrorist, technical, intelligence), particularly heightened overseas. For those agencies with particularly sensitive OCONUS threats, the issuance, holding, and/or use of PIV credentials with full technical capabilities as described herein may result in unacceptably high risk. In such cases of extant risk (e.g., to facilities, individuals, operations, the national interest, or the national security), by the presence and/or use of full-capability PIV credentials, the Secretary of Agriculture may issue a select number of maximum security badges that do not contain (or otherwise do not fully support) the wireless and/or biometric capabilities otherwise required/referenced herein. To the greatest extent practicable, agencies should minimize the number of requests for such special-risk security badges so as to support inter-agency interoperability and the President's policy. Use of other risk-mitigating technical (e.g., high-assurance on-off switches for the wireless capability) and procedural mechanisms in such situations is preferable, and as such is also explicitly permitted and encouraged. As protective

security technology advances, this need for this provision will be re-assessed as the standard undergoes the normal review and update process."

Since foreign national employees and contractors may not have lived in the U.S. long enough for a background investigation to be meaningful, USDA should conduct an equivalent investigation, consistent with requirements of this Manual. OMB will establish an interagency working group to explore whether guidance is necessary with respect to background investigations for foreign national employees and contractors. Pending receipt of OMB guidance, if any, agencies shall at a minimum complete a National Agency Check with Inquiries (NACI) for foreign national employees and contractors who have lived in the U.S. continuously for the past 5 years prior to employment. Agencies shall contact the Personnel and Document Security Division (PDSD), and the Office of Security Services (OSS) for guidance on conducting background investigations for foreign national employees and contractors who have not lived in the U.S. continuously for the past five years prior to employment.

5. CREDENTIALING STANDARDS

a. HSPD-12 Minimum PIV Card Credentialing Standards. In accordance with OPM guidelines, a PIV card will not be issued to an individual if any of the following applies:

(1) The individual is known to be or reasonably suspected of being a terrorist;

(2) The employer is unable to verify the individual's claimed identity;

(3) There is reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity;

(4) There is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information;

(5) There is a reasonable basis to believe the individual will use an identity credential outside the workplace or inappropriately; or

(6) There is a reasonable basis to believe the individual will use Federally-controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

b. Supplemental PIV Card Credentialing Standards: USDA may work with individuals who do not require a suitability determination or a security clearance. In such cases, there is flexibility to apply supplemental

credentialing standards in addition to the six basic standards in the previous section. These supplemental standards are intended to ensure that the grant of a PIV card to an individual does not create unacceptable risk, when the individual is not subject to an adjudication of suitability for employment in the competitive service under 5 CFR part 731, or qualification for employment in the excepted service under 5 CFR part 302 or under a similar authority, or of eligibility for access to classified information under E.O. 12968. These standards may be applied based on the risk associated with the position or work on the contract.

An agency may consider denying or revoking a PIV card to an individual based on one of these supplemental credentialing standards. In the following standards, an "unacceptable risk" refers to an unacceptable risk to life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial, or medical records; or to the privacy of data subjects.

(1) There is a reasonable basis to believe, based on the individual's misconduct or negligence in employment, that issuance of a PIV card poses an unacceptable risk;

(2) There is a reasonable basis to believe, based on the individual's criminal or dishonest conduct, that issuance of a PIV card poses an unacceptable risk;

(3) There is a reasonable basis to believe, based on the individual's material, intentional false statement, deception, or fraud in connection with Federal or contract employment, that issuance of a PIV card poses an unacceptable risk;

(4) There is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

(5) There is a reasonable basis to believe, based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

(6) A statutory or regulatory bar prevents the individual's contract employment; or would prevent Federal employment under circumstances that furnish a reasonable basis to believe that issuance of a PIV card poses and unacceptable risk; or

(7) The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

6. RECIPROCITY OF CREDENTIALING DETERMINATIONS

OMB guidance requires agencies to accept PIV card credentialing determination for a person transferring from another agency when the possession of a valid Federal identity credential can be verified by the person's former agency and the individual has undergone the required NACI or other suitability or National Security investigation at the person's former agency.

At the agency's discretion, a person may be ineligible for a PIV card when the former employing agency (1) determined he or she is unsuitable for employment in the competitive service, (2) denied (or revoked) his or her security clearance, or (3) disqualified him or her from an appointment in the excepted service or from working on a Federal contract. Credentialing determinations are maintained by the granting agency in the Identity Management System (IDMS). This system will allow agencies to certify each other the HSPD-12 credentialing of employees, and contractor employees.

If a person's eligibility for a PIV card is unfavorably adjudicated for reasons other than standards 1-6 of Section 5, sub-section a, and the person moves to a lower-risk position, the gaining agency or office may reconsider the person's eligibility for a PIV card.

CHAPTER 2

PIV-I

1. PIV-I APPLICABILITY

PIV-I requires the implementation of registration, identity proofing, and issuance procedures in line with the requirements of FIPS 201-1. To comply with this requirement, agencies must adopt and implement DR 4620-002 and DM 4620-002.

According to FIPS 201-1 PIV-I applies to employees and contractors requiring routine access to Federally-controlled facilities or information systems, who have begun work on or after October 27, 2005. USDA has determined that all full time employees (FTEs) will require a LincPass, while part time employees' and contractors' need for a LincPass (USDA's PIV-I and II compliant credential), will be assessed based on the level of access required using the risk assessment tool described in Appendix D of this document, LincPass Distribution Risk Assessment.

All individuals shall follow the procedures outlined in the Appendices to apply for and receive their credentials. Agencies will continue to issue existing badges using PIV-I processes until the USAccess system is implemented. The processes for application, registration, and issuance will change with this solution, as well as roles and responsibilities. The PIV-II procedures and processes utilizing USAccess are discussed in detail in Chapter 3.

2. PRIVACY POLICY

HSPD-12 explicitly states that "protect[ing] personal privacy" is a requirement of the PIV system. As such, agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in FIPS 201-1, as well as those specified in Federal privacy laws and policies including but not limited to the E-Government Act of 2002, the Privacy Act of 1974, and OMB Memorandum M-03-22 (OMB322), as applicable.

Background investigation records are subject to the Privacy Act. Agencies must ensure those records are:

a. Secured against unauthorized access.

b. Accessed by only those whose official duties require such access.

c. Stored in a locked metal file cabinet or secure room.

Agencies must also:

a. Establish procedures to allow employees or their designated representatives access to their own records, while ensuring that the records remain subject to agency control at all times.

b. Ensure that those authorized to access personnel records subject to the Privacy Act understand how to apply the Act's restrictions on disclosing information from a system of records.

c. Coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV system.

See OPM's Guide to Personnel Recordkeeping, Chapters 1 and 6, at: http://www.opm.gov/feddata/recguide.pdf for instructions on proper safeguarding of personnel records, and DR 3080, Records Management, at: www.ocio.usda.gov/records/doc/DR3080-001.htm.

Agencies with active roles in the HSPD-12 processes must ensure the following items are secured in a GSA-approved Class V container with a Kaba Mas (formerly known as Mas Hamilton) X09 lock:

a. Plastic stock used to make ID credentials

b. ID credentials awaiting destruction

c. ID credentials not in the personal custody of authorized users

3. BACKGROUND INVESTIGATION REQUIREMENTS

a. A NACI is the minimum background investigation that must be performed for all individuals to whom this Directive applies, except when the position requires a more in-depth OPM or National Security community background investigation (OPM/NS BI). In such cases the OPM/NS BI shall be scheduled in lieu of the NACI through the Personnel and Document Security Division (PDSD).

The above requirement may also be met by referencing a previous favorably adjudicated NACI or other OPM/NS BI. Agency human resources offices can meet the above requirement by completing the SF-75, Request for Preliminary Employment Data, Section K, Security Data, for federal employees transferring to the Department. Applicants experiencing a break in Federal service exceeding two years must undergo a new NACI.

b. Agencies are responsible for ensuring proper position sensitivity designation

for employees and contractors, and completion of background investigations consistent with those designations. Agencies must also ensure that periodic reinvestigations are scheduled as required through PDSD.

c. Agencies will submit the SF-85, Questionnaire for Non-Sensitive Positions, and related documents needed to conduct an NACI, directly to OPM and make final PIV identity and suitability determinations on all persons serving in low-risk or non-sensitive positions.

d. Agencies may utilize the Enrollment Station for submitting the FBI fingerprint check to OPM. The Applicant must be sponsored in the USAccess system prior to using the Enrollment Station to submit the fingerprint check. If an agency requires a pre-hiring decision fingerprint check for new employees, they may continue to follow their current processes for obtaining and submitting fingerprint checks instead of submitting the fingerprint check via the Enrollment Station.

e. USDA agencies may issue a provisional credential after successful adjudication of the FBI fingerprint check. Completion and successful adjudication of the final NACI results or OPM/NS BI are still required. Upon completion of a background investigation, and at the time of determination of suitability, eligibility for access to classified information under E.O. 12968, or to work on a contract, should be made by the agency with a final credentialing determination. Alternatively, agencies may issue a PIV card after a single and final credentialing determination is made based on a completed background investigation, eligibility for access to classified information under E.O. 12968, or qualification for an appointment in the expected service or to work on a contract, is made on the same person.

f. Applicants shall submit SF-85 forms via OPM's Electronic Questionnaire for Investigations Processing (a USDA accepted background investigation process) system located on the OPM secure Web site when available. Use of a USDA accepted background investigation process must be facilitated by agency human resources or other designated representatives. Completing a USDA accepted background investigation process Web-based security questionnaires will lead to improved processing time of all types of investigations and dramatically reduce the overall error and rejection rates of federal security questionnaires.

g. In the case of non-US citizens at U.S.-Based Locations and in U.S. Territories, immigration status and employment authorization of non-US citizens must be verified with the Department of Homeland Security (DHS) in accordance with OMB Memorandum 07-21. Acceptable DHS credentials to prove employment authorizations include, but are not limited to:

- Unexpired Permanent Resident Card (I-551)

- Unexpired Employment Authorization Document (I-766)
- Unexpired foreign passport with a valid I-94 or I-94A for a class of admission that permits employment.

(1) For non-U.S. citizens in the U.S. or U.S. territory for 3 years or more, a background investigation (NACI or equivalent) must be initiated after immigration status and employment authorization have been verified

(2) For non-U.S citizens in the U.S. or U.S territory for less than three years, agencies may delay the background investigation until the individual has been in the U.S or U.S. territory for at least three years. Before a PIV card may be issued to a non-U.S. citizen, the individual's immigration status and employment authorization must be verified, an FBI finger print based on criminal history must be completed, and a check must be made of Specially Designated Nationals (SDN) and Blocked Persons List. If the agency decides to delay the background investigation, the agency may request the following national agency checks:

- FBI Investigation Files (name check search)
- Central Intelligence Agency (CIA)
- Department of State Security
- Citizen and Immigration Services Check (Former INS)

(3) In the case of non-US citizens at foreign locations, agencies must initiate the completion of a background investigation before applying the credentialing standards. However, the type of background investigation may vary based on the standing reciprocity treaties concerning identity assurance that exist between the United States and its Allies with the host country. In most cases, OPM will not be able to conduct a NACI, unless the non-U.S. citizen is or has been residing in the United States.

(4) For those non-U.S. citizens where NACI or equivalent cannot be performed, an alternative facility access identity credential may be issued at the discretion of the Department of State Chief of Mission Authority, Department of Defense Installation Commander, and/or other agency official as appropriate based on a risk determination

See OSS guidance for instructions on scheduling and adjudicating background investigations at www.usda.gov/da/pdsd.

4. REGISTRATION, IDENTITY PROOFING, AND CREDENTIAL ISSUANCE

The PIV-I process contains critical roles associated with the identity proofing, registration, and issuance process. These roles may be collateral duties assigned to personnel who have other primary duties. The PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.

a. Roles and Responsibilities

The roles and responsibilities initially defined for the PIV-I process have been redefined for PIV-II. See Chapter 3 for more information on PIV-II roles and responsibilities.

b. Registration, Identity Proofing, and Issuance Procedures

The procedures initially defined for the PIV-I process have been redefined for PIV-II. See Appendix C for more information on PIV-II procedures.

c. Adjudication

(1) When making a PIV eligibility determination, the Adjudicator must find whether or not the identity provided to the Sponsor and Registrar during the registration process is the Applicant's true identity. The Adjudicator will consult with the federal Applicant or employee's servicing human resources office before making a final determination whether to deny or revoke a credential.

If the adjudication confirms the individual's true identity but reveals potentially disqualifying information that involve criteria 1 through 8 below, an adjudication under Title 5, C.F.R. Part 731 shall be conducted. Title, 5 C.F.R. Part 731 criteria are:

(a) Misconduct or negligence in employment

(b) Criminal or dishonest conduct

(c) Material, intentional false statement or deception or fraud in examination or appointment

(d) Refusal to furnish testimony as required by §5.4 of Title 5, C.F.R.

(e) Alcohol abuse of a nature and duration which suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of others

(f) Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation

(g) Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force

(h) Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question

(2) When making a suitability determination under Title 5 C.F.R. Part 731, the following factors shall be considered to the extent they are deemed pertinent to the individual case:

(a) The nature of the position for which the person is applying or in which the person is employed

(b) The nature and seriousness of the conduct

(c) The circumstances surrounding the conduct

(d) The recency of the conduct

(e) The age of the person involved at the time of the conduct

(f) Contributing societal conditions

(g) The absence or presence of rehabilitation or efforts toward rehabilitation

d. Appeal Procedures for Denial or Revocation of Credential

(1) Appeal Rights for Federal Service Applicants

When the Adjudicator determines that a Applicant has not provided his or her true identity during the registration process or is found unsuitable, and the determination results in a decision by the agency to withdraw an employment offer, or remove the employee from the federal service, the procedures and appeals rights of either 5 CFR Part 731, Subparts D and E (Suitability), 5 CFR Part 315, Subpart H (Probationary Employees), or 5 CFR Part 752, Subparts D through F (Adverse Actions) will be followed, depending on the employment status of the federal service Applicant, appointee, or employee. Employees who are removed from federal service are entitled to dispute this action using applicable grievance, appeal, or complaint procedures available under Federal regulations, Departmental directives, or collective bargaining agreement (if the employee is covered).

(2) Appeal Rights for Contract Applicants

(a) Notice of Proposed Action - When the Adjudicator determines that an Applicant has not provided his or her true identity or is found unsuitable, the Adjudicator shall provide the Applicant reasonable notice of the determination including the reason(s) the Applicant has been determined to not have provided his or her true identity or is otherwise unsuitable. The notice shall state the specific reasons for the determination, and that the individual has the right to answer the notice in writing. The notice shall inform the Applicant of the time limits for response, as well as the address to which such response should be made.

(b) Answer - The Applicant may respond to the determination in writing and furnish documentation that addresses the validity, truthfulness, and/or completeness of the specific reasons for the determination in support of the response.

(c) Decision – After consideration of the proposed determination and any documentation submitted by the Applicant for reconsideration of the proposed determination, the Agency Head/Staff Office Director or his/her designee, will issue a written decision to the Contracting Officer (CO), who relays the decision to the Applicant's company Program Manager and the Contracting Officer's Technical Representative (COTR). The CO will notify the company that the Applicant was found unsuitable to work on a USDA contract based on suitability guidelines. The company is responsible for notifying the Applicant of the decision and removing the individual from the worksite. The COTR is responsible for ensuring the action is accomplished without delay. Specific details regarding the suitability issues will not be provided to the CO, the company, the COTR or the Program Manager, in an effort to protect the Applicant's privacy. The reconsideration decision will be final and is not subject to appeal.

e. Record Retention

(1) The SF-85, SF-85P, SF-86, OF-306, SF-87, FD-258, and summaries of reports and other records reflecting the processing of the NACI or OPM/NS BI, exclusive of copies of investigative reports furnished by the investigative agency: Destroy upon notification of death or not later than five years after separation or transfer of employee or no later than five years after contract relationship expires, which ever is applicable.

(2) Investigative reports and related documents furnished to agencies by investigative organizations for use in making PIV ID credential eligibility determinations: Destroy in accordance with the investigating

agency instructions.

(3) Appeal records related to unsuccessful adjudications: Destroy no sooner than 4 years but no later than seven years after final appeal decision. See GSA Records Schedule 1 and 18 at: http://www.archives.gov/records-mgmt/ardor/records-schedules.html and DR 3080-001, Records Management, at: http://www.ocio.usda.gov/directives/doc/DR3080-001.pdf.

5. EXPIRATION DATE REQUIREMENTS

All PIV credentials issued to the USDA must have an expiration date printed on them. The expiration date for all credentials must be five years or less from the date of issuance. PIV credentials for contractors must expire at the end of the contract period of performance.

All badges issued to applicable employees and contractors must be replaced with PIV-compliant credentials no later than October 27, 2009.

6. TEMPORARY BADGES

USDA has identified categories of individuals, temporary employees or contractors, guests, volunteers, student interns, and occasional visitors, who will not require a LincPass. These individuals, however, may need badges to gain access to facilities but do not require secure access. These individuals will have limited access to such places as the front entrance of the facility, their immediate workspace, and open areas such as a cafeteria, snack bar, employee break room, restroom, and similar open areas, as directed and controlled by the facility. Agencies may choose to implement stricter requirements at their own discretion following the LincPass Distribution Risk Assessment. See Appendix E for more information on the types of credentials/badges USDA issues.

a. Site Badge

A Site badge is issued locally by the facility to persons that do not require a LincPass but need access to the facility or information system to conduct temporary work. Also, a site badge is issued to individuals who require a LincPass after having fingerprints taken and waiting for credential to be printed and returned for activation.

b. Visitor Badge

This type of card can be either a plastic card turned in after the visit and

sequentially numbered, or a paper tag that can be worn and disposed of upon completion of the visit. The paper or plastic badge has the expiration date clearly visible. The maximum issuance for this type of badge is 24 hours, and requires continuous escort.

In addition, should an employee or contractor forget their credential on a particular day, they will be issued a visitor badge after their identity is confirmed.

7. CONTRACTING IMPACTS

a. All contractors must abide by the identity proofing and registration requirements outlined in Chapter 2, Section 4 above. USDA contract statements of work must indicate that all contractors requiring routine access to Federally-controlled facilities or information systems must go through the identity proofing and registration process, and must have been successfully identity proofed, and have a successfully adjudicated NACI or OPM/NS BI to serve on the contract.

b. Contractor ID credentials will be issued after they have been successfully identity proofed, and upon a successfully adjudicated NACI or OPM/NS BI. All contracts must specify periods of performance. Contractors must, by contract law, renew their credentials after 5 years if they have not yet reached the end of their period of performance.

c. Certain PIV language must be implemented in all contracts. This language is found in FAR Subpart 4.13, Personal Identity Verification of Contractor Personnel. HSPD-12 clauses include FAR Clause 52.204-9 and AGAR Clause 452.204-71. AGAR Advisory 81, Common Identification Standard for Contractors, contains additional HSPD-12 procurement guidance.

8. AUDIT AND RECORDS MANAGEMENT

The Office of Inspector General has responsibility for auditing identity proofing and registration records. As such, all agencies should be prepared for such reviews.

Agencies must comply with DR 3080-001, “Records Management,” for the creation, maintenance, use, and disposition of all records associated with the PIV process.

9. USE OF APPROVED FORMS

To comply with the Paperwork Reduction Act (PRA) of 1995, all agencies will be required to use OMB approved forms throughout the identity proofing and registration process. Most of these forms are standard Federal Government-wide

forms that have been available for many years. In addition to the Government-wide forms, the USDA has created an additional PIV specific form that will fulfill the information gathering requirements of the PIV program. The following is a list of approved forms for use in the PIV-I process:

a.	AD-1197:	PIV-I Request and Issuance Approval Form or OMB-approved equivalent (see Appendix I).
b.	FD-258:	Fingerprint Chart used to conduct contractor FBI fingerprint checks.
c.	OF-306:	Declaration for Federal Employment
d.	OF-612:	Optional Application for Federal Employment
e.	OPM OFI-79A:	Report of Agency Adjudicative Action on OPM Personnel Investigations
f.	Standard Form (SF) 85:	OPM Questionnaire for Non-Sensitive Positions (to be completed using a USDA accepted background investigation process when available)
g.	SF 85P:	OPM Questionnaire for Public Trust Positions (to be completed using a USDA accepted background investigation process)
h.	SF 86:	OPM Questionnaire for National Security Positions (to be completed using a USDA accepted background investigation process)
i.	SF 87:	Fingerprint Chart used to conduct FBI fingerprint checks for federal appointees and employees and Applicants for federal employment.

10. REPORTING REQUIREMENTS

Agencies are required to submit quarterly and annual reports on their credential

programs to ensure controls are in place for tracking all credentials. Agencies must submit the following reports to OSS within 15 days of the end of each quarter and the fiscal year:

a. Number of credentials issued during designated period

b. Number of credentials renewed during designated period

c. Number of credentials lost during designated period

d. Number of credentials stolen during designated period

e. Number of credentials revoked during designated period

f. Number of credentials suspended during designated period

g. Number of credentials retired during designated period

h. Number of credentials expired during designated period

Beginning on March 1, 2007 and each quarter thereafter, agencies are required to post a report on number of credentials issued on their public websites per OMB Memorandum M-07-06. This memorandum provides the guidance for reporting the number of credentials issued by quarter and includes the report template.

CHAPTER 3

PIV-II

1. PIV-II OVERVIEW

PIV-II is the implementation phase that meets the technical interoperability requirements of HSPD-12. Specifically, PIV-II addresses the technical infrastructure for providing interoperable credentials for federal employees and contractors. All authentication mechanisms described in FIPS 201-1 are to be met with the use of integrated circuit cards.

FIPS 201-1 describes minimum technical requirements for the PIV-II-compliant credentials. These requirements include interfacing specifications, cryptographic specifications, PKI and certificate specifications, card topology specifications, and biometric data specifications. The PIV-II-compliant credentials issued will be used to control physical access to all Federally controlled facilities and logical access to all Federally controlled information systems through a contact or contactless interface. 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.

For PIV-II, the USDA will be using the USAccess system, a system-based model with increased functionality to improve efficiency and accuracy in processing PIV applications. A planned rollout to USDA employees and contractors will be phased in by organization and geographic location. PIV-II will include three new logical subsystems:

a. PIV Front-End Subsystem - PIV credential and biometric readers, and Personal Identification Number (PIN) input device. The PIV credential holder interacts with the front-end subsystem to gain physical or logical access to the desired Federal resource.

b. Credential Issuance and Management Subsystem - the components responsible for identity proofing and registration, card and key issuance and management, and various repositories and services required as part of the verification infrastructure.

c. Access Control Subsystem – the physical and logical access control systems and authorization data.

2. PIV-II APPLICABILITY

PIV-II applies to all full-time employees, contractors, and others assigned to or associated with the agency who require routine access to federally controlled facilities and/or information systems. Applicability to other individuals will be based on a LincPass risk assessment and is subject to rule making procedures. PIV-II applies to the facilities and information systems as defined in FAR Subpart 2.1, Definitions. Note: The information in Chapter 2, Sections 2, 3, 4c, 4d, 4e, 5, 6, 7, 8, 9, and 10 apply to PIV-II processes and procedures.

3. REGISTRATION, IDENTITY PROOFING, CREDENTIAL ISSUANCE, AND REVOCATION

The PIV-II process contains critical roles associated with the identity proofing, registration, and issuance process. These roles may be collateral duties assigned to personnel who have other primary duties. The PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.

The following roles shall be employed for identity proofing, registration, and issuance prior to complete implementation of USAccess system. See Appendix C for more detailed information on the PIV-II processes.

a. Roles and Responsibilities

(1) Applicant. The Applicant is an individual requesting a credential from an agency that is a participant in the USAccess system. Applicant responsibilities include:

(a) Provide Sponsor with any necessary information.

(b) If no Background Investigation completed or in progress, input information into e-QIP (if available) or fill out the appropriate SF-8X form.

(c) Submit fingerprints for a background check.

(d) Schedule an enrollment appointment.

(e) Appear for the enrollment appointment at the time and place scheduled.

(f) Provide the Registrar with two I-9 listed identity documents.

(g) Submit to a digital photo taken by the Registrar.

(h) Submit 10 rolled fingerprints.

(i) Digitally sign the enrollment package.

(j) Pick up the credential at the specified time and place.

(k) Take the credential to an Activation station to activate it via biometric verification.

(l) Set a PIN for the credential at the Activation Station.

(m) Provide a digital signature.

(n) Complete IT Security Awareness Training.

(2) Sponsor. The Sponsor is the employer or agency official responsible for authorizing an individual to apply for a credential, who has undergone Sponsor training, and is designated to perform Sponsor functions. In the case of contractor employees, the Sponsor may be the COR, COTR, or other designated program official. Sponsor responsibilities include:

(a) Enter Applicant's information into EmpowHR or other HR System.

(b) For part time employees and non-employees, determine if an Applicant needs a LincPass utilizing the Risk Assessment Tool.

(c) Determine if Applicants already have favorably adjudicated background investigations via OPM for employees or through prior agency HR or Security offices for contractors.

(d) If (c) is no, set up Applicant for a USDA accepted background investigation process, or review the Applicant's SF-85, SF 85P or SF-86, Questionnaire for Non-Sensitive Positions, and OF-306, Declaration for Federal Employment.

(e) Modify Applicant's record based on updates to user status and relevant information.

(f) Suspend or revoke LincPass via EmpowHR or USAccess.

(g) Recover revoked credentials and send to the Security Officer for destruction.

(h) Recover suspended credentials and sent to the Security Officer for

secure storage pending resolution of issue(s).

(i) Initiate re-enrollments for current or previous cardholders.

(3) Registrar. The Registrar is an individual responsible for identify proofing the Applicant, as well as capturing biographic information, digital photo, and biometrics. The Registrar's responsibilities include:

(a) Manage schedule for enrollment workstations in case of scheduling conflicts.

(b) Answer any privacy or system related questions that an Applicant may have.

(c) Locate and open the Applicant's information, and verify the information with the Applicant.

(d) Contact the Sponsor if the Applicant's record can not be found in the system to investigate and resolve the problem.

(e) Verify and scan the Applicant's two identity source (I-9) documents.

(f) Enter FBI-required Applicant data.

(g) Capture the Applicant's facial image in the system via a digital photograph.

(h) Capture ten rolled fingerprints into the system.

(i) Verify the primary and secondary fingerprints against the minutiae to ensure that the templates will work when put on the credential.

(j) Flag any issues during enrollment.

(k) Digitally sign and send enrollment package to Credential Printing Facility, and inform Applicant of next steps (i.e. credential issuance and activation process).

(4) U.S. Office of Personnel Management. OPM is responsible for coordinating the FBI fingerprint check, when applicable, and conducting the NACI and background investigation. A direct link from the Enrollment Station to the FBI for submitting fingerprints will be implemented in the near future, but it is the individual agency's decision as to whether to utilize the enrollment station for submitting fingerprints to OPM or to keep using current processes.

(5) Agency Adjudicator. The agency Adjudicator is a Government employee of the sponsoring agency who adjudicates or resolves any issues or failures of the background check process and gives the notification to print. A contractor employee may recommend how to adjudicate a background investigation and record the results in the HSPD-12 system, however a federal employee must sign off on the recommendation first. Agency Adjudicator responsibilities include:

(a) Receive manual reports on background checks.

(b) Confirm NACI or FBI checks, denial of credential if "fail" results.

(c) Respond to inquires on adjudication status from Applicants.

(d) Adjudicate final background investigation results.

(e) Update OPF/contract file or ensure agency receives appropriate documentation.

(6) Issuer/Activator. The Issuer/Activator is the individual responsible for processing credential activations. The Issuer/Activator verifies that the Applicant is the person to whom the credentials are to be issued and guides the Applicant through the issuance process.

Most activation stations will be unattended, meaning that Applicants will use the system without assistance to activate their credentials. In the event that there is an issue causing the unattended activation to fail, the Issuer/Activator will assist the Applicant in completing the activation, or collect the credential, note the issue in the system, and flag the record for issue resolution.

Issuer/Activator responsibilities include:

(a) Receive "to-be-activated" credentials from issuing station, signs for packages (dependent on shipping model).

(b) Log credential into the system, sending out electronic notifications to the Applicants (TBD).

(c) Control secure storage of credentials in a locked safe, logging all action items taken into or out of the safe.

(d) Hand the credential to the individual after verifying their ID.

(e) Verify that the Applicant information in the system and credential display information are correct.

(f) Visually check the Applicant's facial image against the IDMS photo and the LincPass photo to verify that Applicant information and credential display info match if there is no fingerprint record.

(g) Flag the credential in the system and note problems with activation.

(h) Retrieve the credential if activation fails.

(7) Agency Role Administrator. The Agency Role Administrator is the individual responsible for managing the agency's Sponsor, Adjudicator, Registrar, and Issuer/Activators. The Agency Role Administrator will verify that the appropriate separation of duty policies are followed and will verify that all the training certification requirements have been met. Agency Role Administrator responsibilities include:

(a) Authority on separation of roles within agency.

(b) Provide written documentation of any allowance involving a combination of roles.

(c) Approve portal privileges for new role holders, verifying separation of duties and training.

(d) Revoke role privileges and portal access for users within the agency when appropriate.

(8) USDA Security Officer. The USDA Security Officer is the individual responsible for maintaining credential security as well as physical building security within USDA. The USDA Security Officer is nominated by the Department. USDA Security Officer responsibilities include:

(a) Access all records in the system.

(b) Delegate authority to designated Security Officers for record access.

(c) Provide oversight to Security Officers to ensure completed

training, certification, and issuance of credentials.

(d) Report to the Agency Role Administrator that designated Security Officers are trained, certified, and credentialed.

(e) Manage employees' and contractors' "credential status" when required.

(f) Grant necessary access privileges when required.

(g) When required, immediately change the status of a credential between active and suspended due to a security related situation.

(h) Investigate incidents with to resolve any discrepancies if requested by agency.

(i) Collect and destroy lost credentials.

(j) When requested, securely send credentials to another Activation Station when a credential is shipped to a location other than where the Applicant is located.

(9) Agency Security Officer. The Agency Security Officer is the individual responsible for maintaining credential security as well as physical building security for their agency. The Agency Security Officer is nominated by the agency. The Agency Security Officer's responsibilities include:

(a) Access records in the system only related to their agency (TBD).

(b) Delegate authority to agency designated Security Officers for record access.

(c) Make final determination on revocations with the Sponsor when required.

(d) Provide oversight to agency Security Officers to ensure completed training, certification, and issuance of credentials.

(e) Report to the Agency Role Administrator that designated Security Officers are trained, certified, and credentialed.

(f) Manage employees and contractors "credential status."

(g) Grant necessary access privileges.

(h) When required, immediately change the status of a credential

between active and suspended due to a security related situation.

(i) Investigate incidents with to resolve any discrepancies.

(j) Collect and destroy revoked credentials.

(10) Security Officer. The Security Officer is the individual responsible for maintaining credential security as well as physical building security for their agency. Security Officer responsibilities include:

(a) Manage employees' and contractors' "credential status."

(b) Investigate incidents with to resolve any discrepancies.

(c) Collect and destroy revoked credentials.

b. In order to assure timely provisioning and deprovisioning of accounts (desktops, eAuthentication, building access, NFC applications, etc), agencies must record hiring and termination events in the appropriate database (e.g., EmpowHR, Payroll/Personnel or NEIS (for non-employees)) as soon as possible, but not later than:

(1) Hiring. Within 3 days.

(2) Termination--hostile situation. Within 3 days if LincPass is retrieved from person; same day if LincPass is not retrieved from person.

(3) Termination--normal situation. Within 3 days.

4. PHYSICAL ACCESS CONTROL SYSTEMS (PACS)

To comply with one of the four tenants of HSPD-12 (rapidly authenticate electronically), USDA has developed and implemented a FIPS 201-1 compliant enterprise PACS infrastructure in order to rapidly provision and deprovision LincPasses (and all USDA issued electronic badges) based on the PIV process. All authentication mechanism standards described in FIPS 201-1 are to be met, by October 2011, as mandated by the Office of Management and Budget (OMB), for all existing legacy and newly installed PACS. All USDA PACS must interface with the USDA enterprise Physical Access Control System (ePACS) infrastructure.

All USDA agencies need to establish implementation plans for this integration for the following scenarios:

a. Continued Use of Existing Compliant PACS
b. Converting an Existing PACS to meet Compliancy
c. Purchase and Install of a new Compliant PACS

Procedures for integrating PACS into ePACS are as follows:

a. Contact the ePACS Program Management Office (PMO) before the integration of an existing PACS or new PACS installation for pre-planning and implementation guidance.

b. Before procuring PACS hardware and software for a new PACS installation the ePACS Cost Benefit Analysis spreadsheet must be filled out to ensure USDA agencies select the most cost effective manner to meet HSPD-12 and ePACS compliance while meeting their operational security needs.

c. Notify the ePACS PMO of any PACS-related hardware/software that is involved in the integration with ePACS or planned to be added to ensure budget numbers are captured for software licensing for the following fiscal year. USDA agencies must submit change requests through their agency Change Control Board (CCB) member. A telephone call to the ePACS Help Desk at 888-212-9309 can provide Agency POC information and answer any other questions that may arise.

d. Review and comply with the GSA Approved Products List when ordering PACS hardware/software or services (implementers).

e. PACS that are chosen must meet not only HSPD-12 compliance and interoperability requirements but also ePACS requirements.

f. Agency's must submit an IT Acquisition Approval Request (AAR) to OSS for approval for all PACS components before purchase and install.

g. Agencies may fall under the OSS AAR for ePACS if they provide an equipment list and scope of work for review and approval to OSS.

h. All compliant PACS must undergo the Certification and Accreditation (C&A) process with System Test & Evaluation (ST&E) if they are not integrated into the ePACS. Contact the Office of the Chief Information Officer (OCIO) Cyber Security Office for C&A requirements and deadlines.

5. LOGICAL ACCESS CONTROL SYSTEMS (LACS)

In compliance with PIV-II, agencies should evaluate existing LACS during FY 2007 as follows:

a. Continued Use of Existing LACS

Existing LACS do not support the use of PIV-II-compliant credentials at an enterprise level. Agencies must continue to integrate applications requiring authentication with the USDA eAuthentication service, and continue to use the existing credential assurance levels as defined in DR 3610-001, "USDA eAuthentication Service."

b. Upgrading Existing LACS

Agencies may have to replace existing computer equipment as the technology reaches the end of its lifecycle. Per DR 3600-000,"USDA Information and Technology Transformation," all proposed USDA information management and technology investments must be evaluated to ensure they align with USDA business goals, objectives of the USDA eGovernment mission, and integrate with and not duplicate USDA and government-wide initiatives. Therefore, all upgrades to existing LACS must be approved by the USDA Chief Information Officer (CIO) to ensure the products will be compatible with the USDA's credential issuance and management system. USDA plans to implement a FIPS 201-1-compliant enterprise-wide LACS infrastructure by October 27, 2009. Agencies should check the status of emerging USDA standards for peripheral devices, keyboards, card readers, etc. before making purchases.

c. Purchase of New LACS

By October 2008, PIV-II-compliant credentials containing a contact chip and digital certificate will be issued. Agencies will make risk-based decisions on what level of assurance they will require for access to their information systems. Based on these assurance level decisions, the purchase of card readers and biometric readers may be required. Per DR 3600-000, "USDA Information and Technology Transformation," all proposed USDA information management and technology investments must be evaluated to ensure they align with USDA business goals, objectives of the USDA eGovernment mission, and integrate with and not duplicate USDA and government-wide initiatives. Therefore, all new LACS purchases must be approved by the CIO. All purchases approved by the CIO must be of products included on the GSA schedule of FIPS 201-1-compliant products and vendors. Products on the GSA schedule have gone through the necessary testing to ensure compliance with the technical and interoperability requirements of PIV-II.

6. LINCPASS BADGE HOLDER

The LincPass must be stored at all times in the approved badge holder, the Logic First Skim-Shield Rigid-2, model LGF001. The approved badge holder is available

for purchase by agencies via a Blanket Purchase Agreement (BPA AG-3142-B-0011). All LincPass badge holders must be ordered using this BPA.

7. LINCPASS DISPLAY

The LincPass should be stored in the approved badge holder and fastened to either an item of clothing or an approved chain or lanyard worn around the neck. The LincPass should be worn above the waist in such a manner that the ID photograph is clearly visible from the front at all times. In cases where a person works in a hazardous environment where it would be unsafe to wear the LincPass in the manner outlined, it is permissible to place the LincPass in a pocket. Once the person leaves the hazardous work area, it must be properly worn and displayed again. Agencies must define the work areas in which it would be unsafe to wear the LincPass as outlined in this section.

CHAPTER 4

TRAINING

Training for HSPD-12 roles (Role Administrators, Sponsors, Registrars, Adjudicators, and Issuer/Activators) will be required. Specific information regarding training will be provided in Appendix F of this document. Appendix G will contain training information for non-PACS facilities.

USAccess provides training modules for HSPD-12 Role Holders. All Role Administrators, Sponsors, Registrars, Adjudicators, Activators, and Security Officers must take training and be certified to perform their duties. These training modules will be in AgLearn and the courses will be incorporated into the appointed role holder's learning plan.

There are 6 training modules with a certification test at the end of each module.

WBT Working Title	**Est. Duration**	**Description**
GSA PIV Sponsor Training	40 minutes	Includes audio, screen shots and SWF movies of the application.
GSA PIV Registrar Training	60 minutes	Includes audio, screen shots, SWF movies, and video
GSA PIV Adjudicator	30 minutes	Audio, screen shots, SWF movie
GSA PIV Activator Training	30 minutes	Includes audio, screenshots, SWF movies, maybe some video
GSA PIV Security Office Training	40 minutes	Includes audio, screen shots,, SWF movies
GSA PIV Role Administrator Training	20 to 30 minutes	Includes, audio, screen shots, SWF movies

Training results will be recorded on AgLearn, in which the Role Administrator and Agency Role Administrator will have access for training management.

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. AD-1197. Request for USDA Identification (ID) Badge (PIV) Request Form.

d. e.Authentication. The process of establishing an individual's identity and determining whether individual Federal employees or contractors are who they say they are.

f. Authorization. Process of giving individuals access to specific areas or systems based on their authentication.

g. Biometric. A measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints, and facial images. A biometric system uses biometric data for authentication purposes.

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

i. Employee. Federal employees as defined by title 5 U.S.C §2105 "Employee," within USDA; or individuals employed by, detailed to or assigned to USDA.

j. e-QIP. The Electronic Questionnaires for Investigations Processing is an Office of Personnel Management (OPM) system that allows for the secure transmission of security questionnaires between government agencies and OPM.

k. e-QIP Tracking Number. Number assigned by e-QIP to each SF-85, 85P, and SF-86. This tracking number must be written on the fingerprint card when it is submitted to OPM in order to bind the fingerprint card to the proper Applicant.

l. Executive Order 10450. Security Requirements for Government Employees.

m. FBI. Federal Bureau of Investigation.

n. FBI Fingerprint Check. FBI National Criminal History Check. This check is an integral part of the NACI, and is the minimum requirement for PIV ID credential

issuance.

o. FD-258. Fingerprint Chart used to conduct contractor FBI fingerprint checks.

p. 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.

q. Identity Management System. One or more systems or applications that manage the identity verification, validation and issuance process. The IDMS software is used by PIV Registrars to enroll Applicants.

r. 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.

s. 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.

t. 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.

u. 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.

v. 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).

w. 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.

x. OF-306. Declaration for Federal Employment.

y. Physical Access Control System (PACS). Protection mechanisms that limit a user's 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).

z. 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.

aa. LincPass Distribution Risk Assessment. The determination of a person's legitimate need for physical/logical access using a PIV ID credential as outlined in HSPD-12 to USDA facilities/information systems, and the requirement to view sensitive information.

bb. Provisional Badge. A LincPass issued on the basis of a favorable adjudication of the fingerprint check only. The LincPass has full PIV-II capabilities but the status of the credential is not changed from provisional to permanent unless and until the full background investigation is favorably adjudicated.

cc. Public Key Infrastructure (PKI). A service that provides cryptographic keys needed to perform digital signature-based identity verification, and to protect communications and storage of sensitive data.

dd. Standard Form (SF)-85. Questionnaire for Non-Sensitive Positions.

ee. Standard Form (SF)-85P. Questionnaire for Public Trust Positions.

ff. Standard Form (SF)-86. Questionnaire for National Security Positions.

gg. Standard Form (SF)-87. Fingerprint Chart used to conduct FBI fingerprint checks for federal appointees and employees and Applicants for federal employment.

hh. Security Office Identifier (SOI). Four-digit number assigned by the U.S. Office of Personnel Management (OPM) to identify the proper federal agency officials to receive reports of investigation, data, or information from OPM.

ii. Site Badge. A badge issued locally by the facility to persons that do not need a LincPass but need access to the facility or information system to conduct temporary work.

jj. Submitting Office Number (SON). Four-digit number assigned by the U.S. Office of Personnel Management (OPM) to offices authorized to submit NACI requests.

kk. Temporary Employee: Temporary, Term, Student, or intern paid or obtaining some sort of benefit directly from USDA.

ll. Visitor Badge. This type of card can be either a plastic card turned in after the visit and sequentially numbered, or a paper tag that can be worn and disposed of upon completion of the visit. These badges will have the expiration date clearly visible. The maximum issuance for this type of badge is 24 hours.

mm. 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.

nn. Visitor. Individual authorized to be in a controlled facility on a short-term and limited or controlled basis.

oo. Volunteer. A non-paid individual working under supervision of USDA.

APPENDIX B

ABBREVIATIONS

BI	Background Investigation
CMS	Card Management System
FIPS	Federal Information Processing Standard
FBI Fingerprint Check	FBI National Criminal History Fingerprint Check
FISMA	Federal Information Security Management Act
HSPD-12	Homeland Security Presidential Directive 12
IDMS	Identity Management System
LACS	Logical Access Control System
MCF	Mission Critical Facility
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NCR	National Capital Region
NIST	National Institutes of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPF	Official Personnel Folder
OPM	Office of Personnel Management
OPM/NS BI	Office of Personnel Management or National Security Community Background Investigation
OSS	Office of Security Services
PACS	Physical Access Control System
PDSD	Personnel and Document Security Division
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification, Part I
PIV-II	Personal Identity Verification, Part II
PKI	Public Key Infrastructure
POC	Point of Contact
SII	Security/Suitability Investigations Index
SOI	Security Office Identifier
SON	Submitting Office Number
SP	Special Publication
USDA	United States Department of Agriculture

APPENDIX C

PIV-II STANDARD OPERATING PROCEDURES

a. Sponsorship

(1) Employee Process

(a) For part time employees, Sponsor uses the Risk Assessment to determine whether the applicant requires a LincPass and checks the appropriate box.

(b) The Sponsor enters the required information for the Employee (also referred to as an Applicant) into EmpowHR or Payroll Personnel (P/P).

(c) The Sponsor initiates a background investigation and enters Applicant in a USDA accepted background investigation process (or initiates background investigation paperwork if a USDA accepted background investigation process is not available).

(d) Applicant enters background information in a USDA accepted background investigation process for investigation (or fills out paperwork).

(2) Contractor Process

(a) COTR uses the Risk Assessment to determine whether the Applicant requires a LincPass and checks the appropriate box.

(b) The Sponsor enters the required information for the Contractor (also referred to as an Applicant) into NEIS.

(c) The Sponsor initiates a background investigation and enters Applicant in a USDA accepted background investigation process (or initiates background investigation paperwork if a USDA accepted background investigation process is not available).

(d) Applicant enters background information in a USDA accepted background investigation process for investigation (or fills out paperwork).

b. Enrollment

(1) The Applicant is sponsored and put into the appropriate (EmpowHR, NEIS or USAccess) system.

(2) The Applicant will be notified by e-mail to schedule an appointment to enroll.

(3) The Applicant schedules an appointment time and location in a web based application.

(4) Upon the arrival of the Applicant to the enrollment station, the Registrar locates and opens the Applicant's information, and verifies the information with the Applicant.

(5) The Registrar validates and scans the Applicant's two identity source (I-9) documents.

(6) The Registrar obtains Applicant's fingerprints and photo, and verifies that the Applicant's fingerprints can be matched to the scanned images that will be used to create the biometric template.

(7) The Registrar verifies all information is correct and complete.

(8) The Applicant signs the enrollment application electronically using personal PIN, PIV credential and fingerprint.

(9) The Registrar completes Applicant's enrollment file and sends to OPM.

c. Adjudication

(1) The Adjudicator receives manual or electronic report on background check.

(2) Confirms NACI or FBI fingerprint checks, adjudicates background investigation results.

(3) Enters results in EmpowHR or USAccess.

d. Card Production

(1) Credential is printed at card production facility.

(2) Credential is shipped to the designated shipping address.

(3) Finalization instructions to activate credential are emailed to the Applicant.

e. Credential Activation and Finalization

Most activation stations will be unattended, meaning that Applicants will use the system without assistance to activate their credentials. In the event that there is an issue causing the unattended activation to fail, the Issuer/Activator will assist the Applicant in completing the activation, or collect the credential, note the issue in the system, and flag the record for issue resolution.

(1) Issuer/Activator verifies identity of Applicant.

(2) The Issuer/Activator retrieves the credential from the storage safe.

(3) Issuer/Activator compares the picture on the credential with the Applicant and provides the credential to the Applicant if they match.

(4) If the Applicant biometric sample matches the biometric read from the credential, the Applicant is authenticated to be the owner of the credential.

(5) The Applicant uses the credential number and system generated PIN (provided to Applicant in an e-mail) to log on to the activation web application.

(6) The Applicant provides the primary fingerprint using the biometric card reader for a 1:1 match in the IDMS database. A successful match will result in the credential being unlocked.

(7) The Endorsement screen appears requiring the Applicant's acknowledgement of agreement to terms and conditions for receipt of the credential

(8) The Applicant sets his/her new PIN which will be 6 to 8 digits in length.

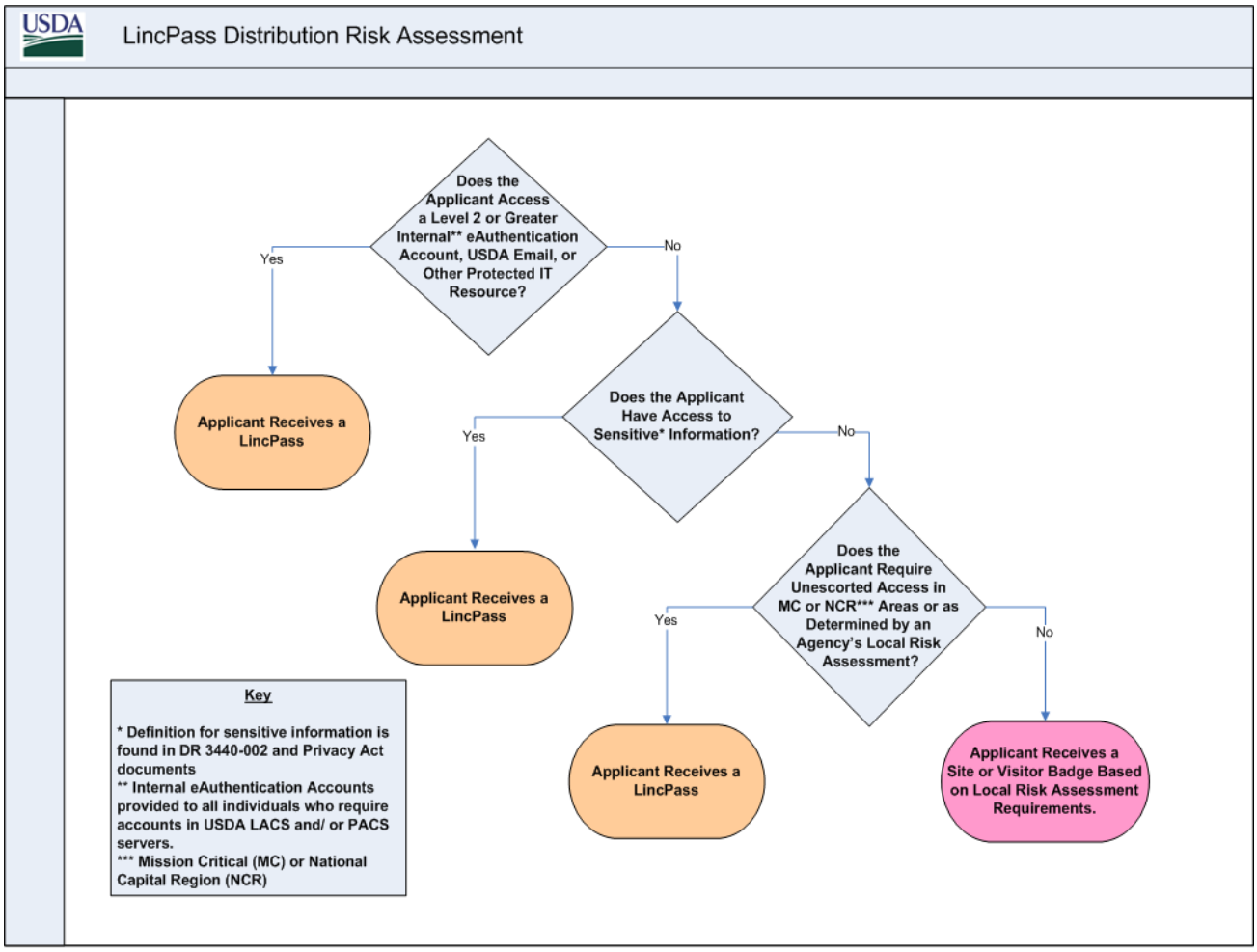
(9) The system encodes the credential with the digital certificates and will display "Successfully Encoded Smart Card" status when finished. The system tests the newly activated LincPass by prompting the Applicant to enter his/her PIN and biometric prints.

(10) The system will prompt the Applicant to remove the LincPass from the Smart Card Reader.

APPENDIX D

FIGURE D-1

LINCPASS DISTRIBUTION RISK ASSESSMENT



DRAFT

EXPLANATION OF CREDENTIAL/BADGE TYPES

a. LincPass. A credential that is issued to Applicants who require level 2 or greater internal eAuthentication account (Internal eAuthentication Accounts provided to all individuals who require accounts in USDA LACS and/or PACS servers), USDA e-mail, or other protected IT resource; 2) who need access to sensitive information (definition for sensitive information is found in DR 3440-002 and Privacy Act documents information); 3) or an Applicant who requires unescorted access in mission critical or National Capital Region (NCR) access areas or as determined by an agency's local risk assessment.

A LincPass can be issued after an Applicant's fingerprints have been submitted and favorable results returned. The credential's expiration date is set for six months while the Applicant's background investigation is being conducted. Once the background investigation is successfully completed then the expiration on the credential will be set according to Chapter 2, Section 5, Expiration Date Requirements.

b. Site Badge. A badge issued locally by the facility to persons who do not require a LincPass but need unaccompanied access to the facility or information system to conduct temporary work. EXAMPLES: Service company employee, such as cafeteria staff, credit union staff, nurse, building management staff, maintenance engineer, day care provider, courier, or repair personnel; or an individual who has officially retired from USDA and receiving retirement benefits.

A site badge can also be issued to an employee or non-employee during the interim period between starting work with USDA and receiving a LincPass.

c. Visitor badge. This type of badge can be either a plastic card turned in after the visit and sequentially numbered, or a paper tag that can be worn and disposed of upon completion of the visit. A paper or plastic badge has the expiration date clearly visible. The maximum issuance for this type of badge is 24 hours, and requires continuous escort. EXAMPLES: a consultant attending a meeting; a LincPass cardholder who does not have their credential with them at the time.

APPENDIX E

PIV-II CREDENTIAL TOPOLOGY AND EXAMPLES OF TEMPORARY BADGES

1. FRONT REQUIREMENTS OF PIV-II CREDENTIAL

a. Zone 1 - Photograph. The photograph shall be placed in the upper left corner and be a full frontal pose from top of the head to shoulder. A minimum of 300 dots per inch (dpi) resolution shall be used. The background will follow recommendations set forth in SP 800-76.

b. Zone 2 - Name. The full name shall be printed directly under the photograph in capital letters.

c. Zone 3 - Not used at this time.

d. Zone 4 - Agency Specific Text. This area is available for optional use by agencies.

e. Zone 5 - Rank. This area is available for optional use.

f. Zone 6 - PDF417 Bar Code. Not used at this time.

g. Zone 7 - Circuit Chip. This chip will encode the biometric and other data linked to the credential.

h. Zone 8 - USDA Affiliation. A USDA affiliation shall be printed on the credential. Some examples of affiliation are: Employee, Contractor, etc.

i. Zone 9 - Header. "United States Government" is default for initial rollout. Agencies may add their own values as long as it is less than the 24 character max.

j. Zone 10 - Organizational Affiliation. Not used at this time.

k. Zone 11 - USDA logo. The USDA logo measuring 1”x ¾” will be printed in this area.

l. Zone 12 - Footer. The footer is the location where the affiliation of Emergency Response Official will be annotated with a red band. All Law Enforcement and Security personnel will have this annotation.

m. Zone 13 - Issue Date. Not used at this time.

n. Zone 14 - Expiration Date. The credential expiration date shall be printed in YYYYMMMDD format.

o. Zone 15 - Color Name Bar. Color coding for employee and other USDA affiliations.

p. Zone 16 - Photo Border. Not used at this time.

q. Zone 17 - Agency Specific Text Area. Not used at this time.

r. Zone 18 - Affiliation Color Code. identifies the color displayed in the color band (e.g., B for Blue, G for Green).

s. Zone 19 - Expiration Date

t. Zone 20 - Organizational Affiliation Abbreviation. Not used at this time

FIGURE E-1

FRONT OF PIV-II CREDENTIAL

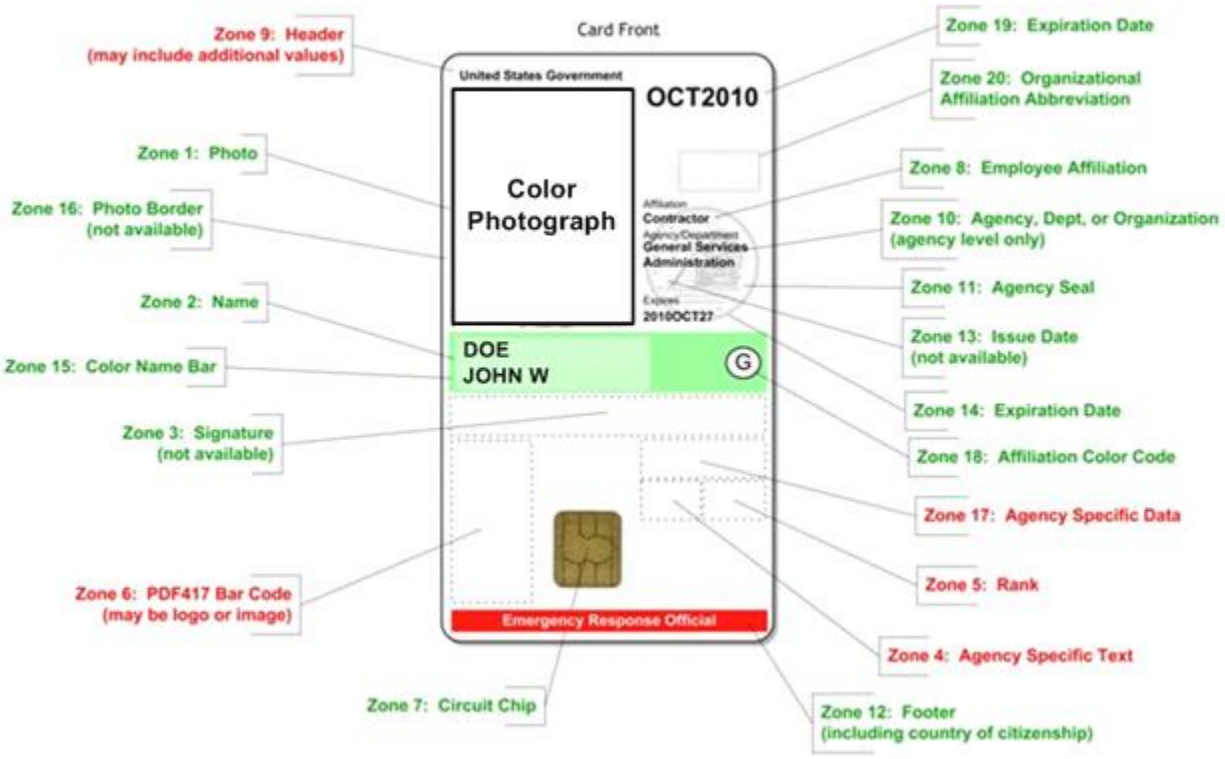
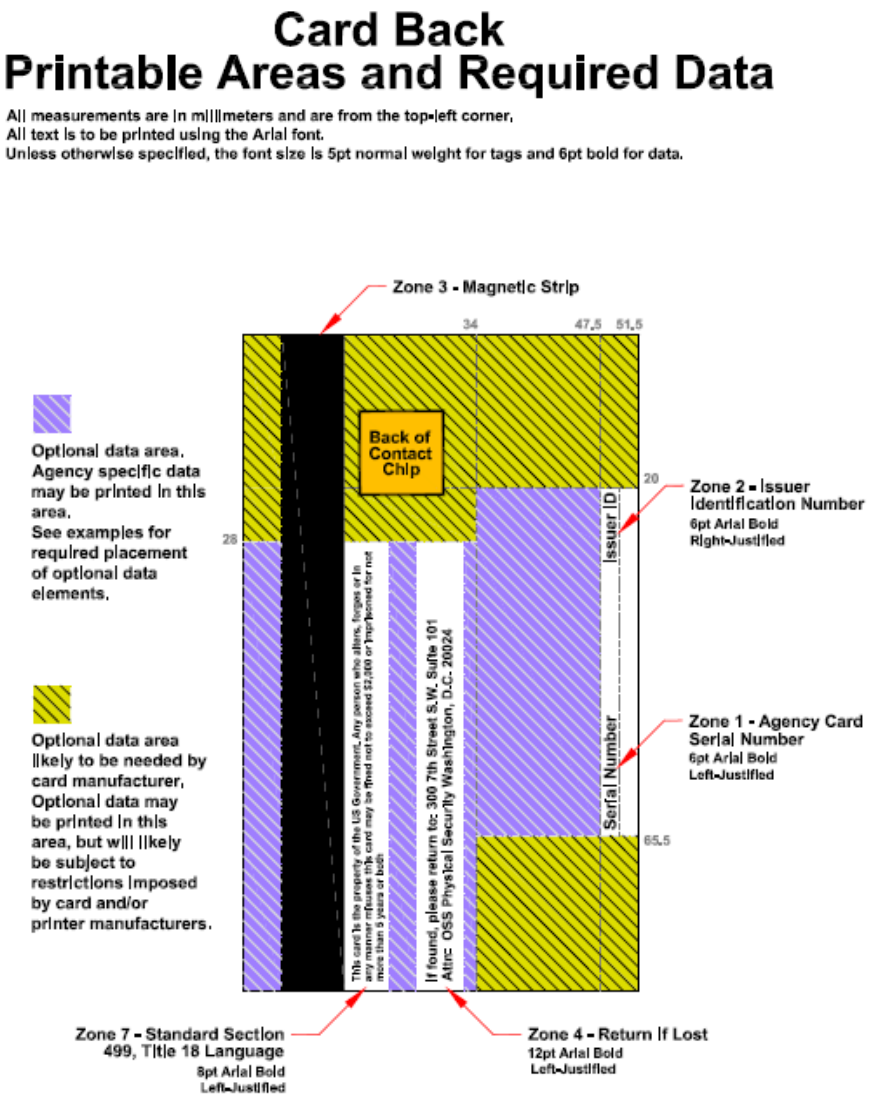


FIGURE E-3

BACK OF PIV-II CREDENTIAL



2. CREDENTIAL BACK PRINTABLE AREAS AND REQUIRED DATA

a. Zone 1. Agency credential serial number (LincPass only)
b. Zone 2. Issuer Identification number (LincPass only)
c. Zone 4. Return Instructions if Found
d. Zone 7. Standard section 499, Title 18 language

FIGURE E-4

EXAMPLE OF LINCPASS

3. USDA LINCPASS COLOR CODING

a. Coding for Federal Employee: White. An individual employed by, detailed to or assigned to USDA under the authority of Title 5 U.S.C §2105 "Employee", and receives government funding for services rendered.

b. Coding for USDA Affiliation—Contractors: Green. An individual under contract (i.e. prime or sub) to USDA, requiring routine unaccompanied access to USDA controlled facilities and/or USDA controlled information systems.

c. Coding for USDA Affiliation—Foreign National: Blue. An individual who is employed by, detailed to, or assigned to USDA but who is not a citizen or permanent resident alien of the U.S. The foreign national color coding takes precedence over the government employee or contractor color designation.

d. Coding for USDA Affiliation—Federal Emergency Response Official. A Federal Emergency Response Official will be annotated with a red band in the footer. All Law Enforcement and Security personnel will have this annotation.

FIGURE E-5

EXAMPLE OF USDA SITE BADGE

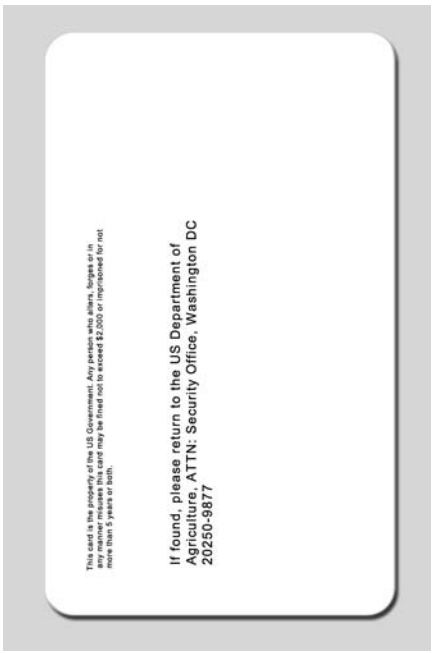


FIGURE E-6

EXAMPLE 1—VISITOR BADGE

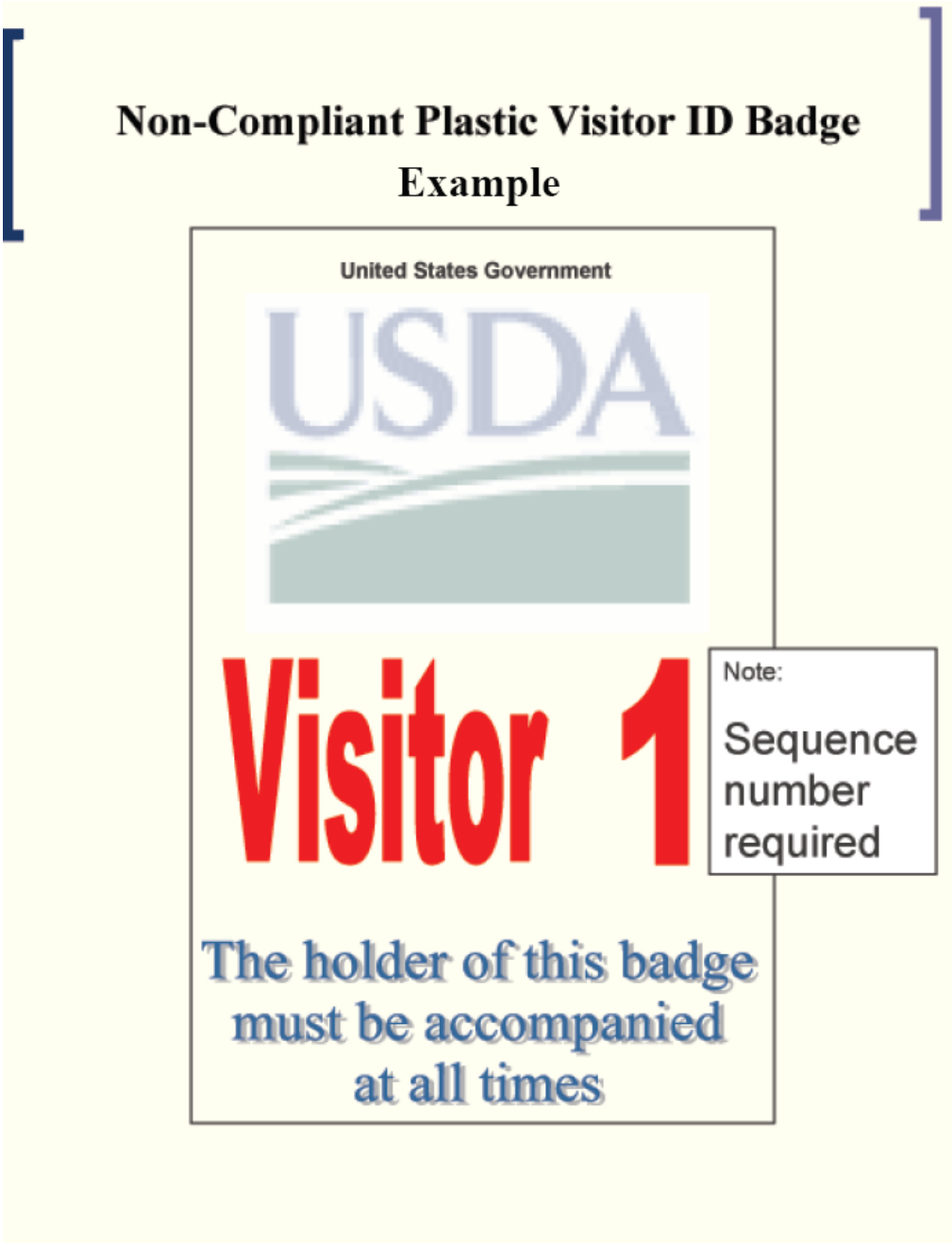


FIGURE E-7

EXAMPLE 2—VISITOR BADGE

Paper Visitor ID Badge

Colors distinguish the day of the week

Example

APPENDIX F

TRAINING FOR PIV-II

References to training type and availability will be included in this appendix on a date to be determined.

APPENDIX G

TRAINING FOR NON-PACS FACILITIES

References to training type and availability will be included in this appendix on a date to be determined

APPENDIX H

ePACS TECHNICAL REQUIREMENTS

The ePACS Technical Requirements will be included in this appendix on a date to be determined

APPENDIX I

FIGURE I-1

FORM AD-1197 may be downloaded from the OCIO web page:

http://www.ocio.usda.gov/forms/doc/AD-1197fill.pdf

APPENDIX J

AMMENDMENTS

1. JULY 31, 2008 AMMENDMENT
   a. Chapter 1, Section 1h - Added additional source of OPM memorandum dated December 17, 2007
   b. Chapter 1, Section 4 – modified 2nd paragraph to remove ambiguity in regards to who requires a LincPass and added language regarding retirees
   c. Chapter 1, Section 5 – Added "Credentialing Standards" section per December 17, 2007 OPM memo
   d. Chapter 1, Section 6 – Added "Reciprocity of Credentialing Determinations" section per December 17, 2008 OPM memo
   e. Chapter 2, Section 3
      (1) Added part d stating agencies have the flexibility to use the enrollment station for fingerprinting or to keep using current process
      (2) Added additional verbiage to part e per OPM memo stating interim credentials may be issued
      (3) Added part g per OPM memo regarding background investigations for non-US citizens
   f. Chapter 2, Section 7 – added 5 year expiration date notice to Chapter 2, Section 7b
   g. Chapter 3, Section 2 – add "full time" to applicability statement
   h. Chapter 3, Section 3a(2) – added statement about who a contractor employee's sponsor may be
   i. Chapter 3, Section 3a(2)(h) – added statement about sending credentials to a Security Officer
   j. Chapter 3, Section 4 – added statement that enrollment station fingerprinting usage is optional
   k. Chapter 3, Section 5 – added statement about a contractor employee's ability to perform Adjudicator functions
   l. Chapter 3, Section 8(j) – Added section about sending credentials to alternate locations
   m. Appendix J – Added new appendix to serve as change log