

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, and affiliates. 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, contractors, and affiliates 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 federal employees and contractors who require access to

federally controlled facilities and/or information systems. Applicability to other individuals will be based on a LincPass risk assessment. 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. 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 pending resolution of issue(s).
 - (i) Initiate re-enrollments for current or previous cardholders.

- (3) Registrar. The Registrar is an individual responsible for identifying 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.
- (5) Agency Adjudicator. The agency Adjudicator is a government employee of the sponsoring agency who resolves any issues or failures of the background check process and gives the notification to print. 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', contractors' and affiliates' "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.

(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, contractors and affiliates "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.

(9) 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', contractors' and affiliates' "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)

All authentication mechanisms described in FIPS 201-1 are to be met with the use of integrated circuit cards. In preparation for PIV-II, agencies are evaluating existing PACS during FY 07 as follows:

a. Continued Use of Existing PACS

FIPS 201-1 mandates that all USDA controlled facilities either use access control, a guard, or some other method to control access to agency facilities. Physical access control will continue to be managed at the agency or facility level, however, the USDA plans to implement a FIPS 201-1-compliant enterprise-wide PACS infrastructure by October 27, 2009 in order to distribute and revoke identity information based on the PIV process, where applicable.

b. Upgrading Existing PACS

The USDA plan calls for the implementation of FIPS 201-1-compliant PACS by October 27, 2011. If any agency/USDA facility plans to replace or install a PACS they must contact OSS Physical Security to coordinate the installation, receive the latest version of GSA approved HSPD-12-compliant systems and a list of vendors who have installed USDA systems successfully. The system that is chosen must be compatible with the USDA Identity Management and Access control enterprise. USDA is currently developing enterprise PACS (ePACS) standards and specifications for dissemination to all agencies and offices to support this migration.

c. Purchase of New PACS

There are numerous options available to install fully compliant low cost access control (from simple low-cost card readers, to fully functional access control portals to automatically grant physical access to USDA facilities). Agencies must only purchase systems from the GSA list of

approved products and ensure the systems will be compatible with the USDA ePACS centralized infrastructure. Products on the GSA schedule have gone through the necessary testing to ensure compliance with the technical and interoperability requirements of PIV-II. All PACS components must be identified on the GSA Approved Products List. Agency's must submit to OSS for approval an IT Acquisition Approval Request for all PACS components before purchase and install. All PACS must undergo the C&A process with ST&E.

5. LOGICAL ACCESS CONTROL SYSTEMS (LACS)

In compliance with PIV-II, agencies should evaluate existing LACS during FY 07 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.

DRAFT

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

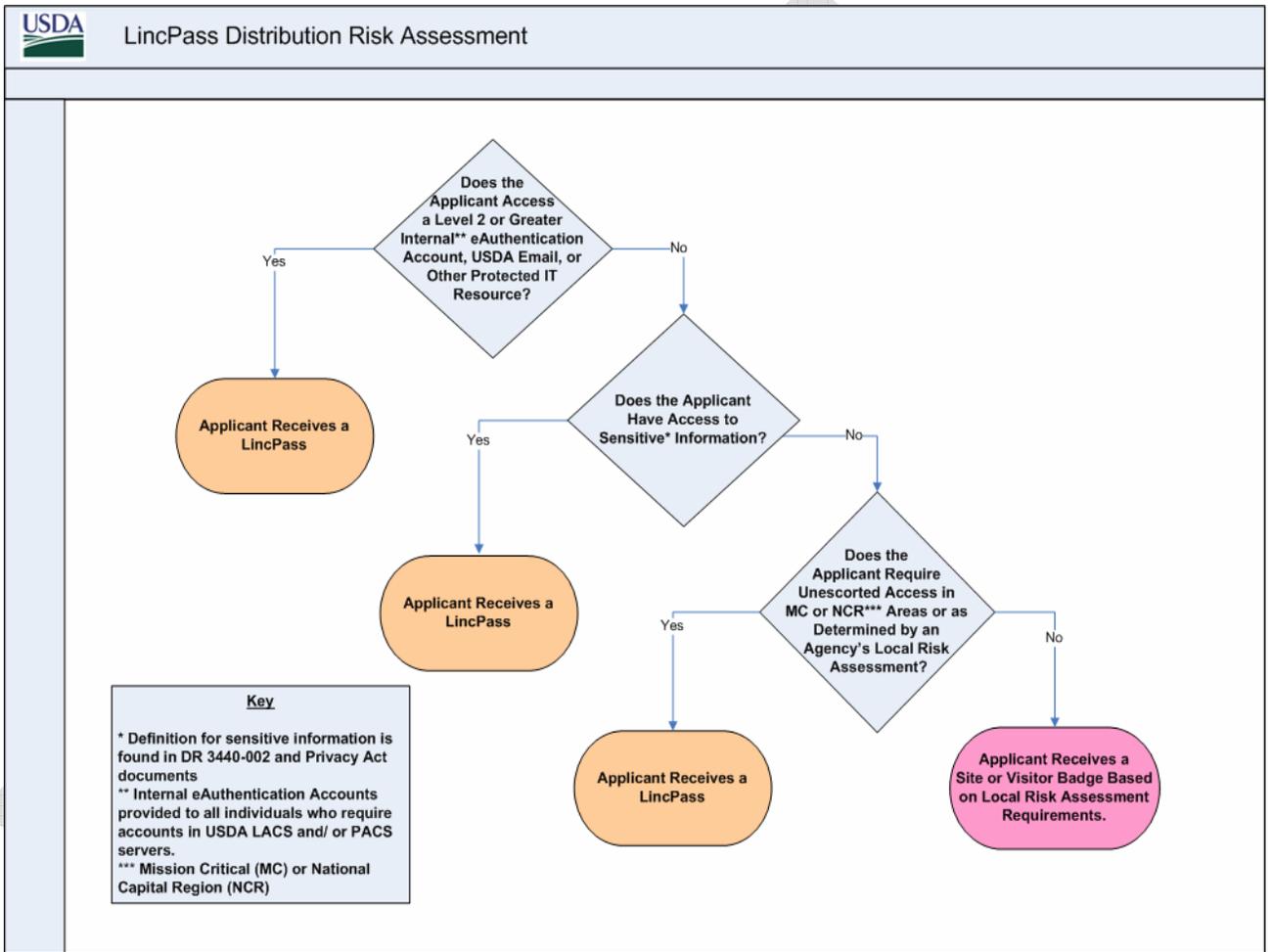
Most activation stations will be unattended, meaning that Applicants will use the system without assistance to activate their credentials. In the event that there is an issue causing the unattended activation to fail, the Issuer/Activator will assist the Applicant in completing the activation, or collect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