

# **Personal Identity Verification II (PIV-II) Business Process Policies and Procedures for Employees**

Prepared for



**United States Department of Agriculture  
Office of Security  
300 7th Street SW, Washington DC 20024**

**Version 1.1**

**August 22, 2007**



## Revision Information

Version	Date	Revision Notes
1.0	07/18/2007	Initial Draft by HSPD-12 Business Process Team
1.1	08/22/2007	(1) Addition of Table 2; Definitions, (2) Grammatical and reformatting edits, (3) Change "Enrollment Officer" to "Registrar", (4) Change the term "Issuer" to Activator/Issuer in the Enrollment, Issuance and Activation processes, (5) Format changes to figures and tables. Changed GSA system to USAccess throughout document, (6) Removal of "Sponsorship and Adjudication" from document title, (7) Removal of Security Officer Revocation 7-4, (8) Change the term "card" to "credential" where applicable.

DRAFT



## Table of Contents

<b>Section 1</b>	<b>Executive Summary .....</b>	<b>1</b>
<b>Section 2</b>	<b>Introduction.....</b>	<b>2</b>
2.1	Background .....	2
2.2	Document Organization .....	2
2.3	Definitions.....	3
<b>Section 3</b>	<b>PIV-II Process Overview.....</b>	<b>7</b>
3.1	Applicant Process.....	7
3.1.1	PART I: Communication .....	9
3.1.2	PART II: Sponsorship .....	9
3.1.3	PART III: Enrollment .....	10
3.1.4	PART IV: Adjudication .....	10
3.1.5	PART V: Issuance.....	11
3.2	HSPD-12 PIV-II Process Overview in EmpowHR.....	12
3.3	HSPD-12 PIV-II Process Overview in Payroll Personnel.....	13
<b>Section 4</b>	<b>Role Administrator .....</b>	<b>14</b>
4.1	Role Administrator.....	15
<b>Section 5</b>	<b>Sponsorship.....</b>	<b>17</b>
5.1	Overview of Sponsorship of Employees .....	18
5.2	EmpowHR Workflows .....	19
5.2.1	First Time Sponsorship of New Employee in EmpowHR .....	19
5.2.2	First-Time Sponsorship of Existing Employee in EmpowHR.....	21
5.2.3	Employee Information Change in EmpowHR .....	23
5.2.4	Employment Status Change in EmpowHR.....	24
5.2.5	Sponsorship Suspension EmpowHR.....	25
5.2.6	Sponsorship Termination in EmpowHR.....	26
5.2.7	Sponsorship Reactivation in EmpowHR .....	28
5.2.8	Employee Card Required Change in EmpowHR.....	29
5.2.9	Employee Other Information Change in EmpowHR .....	31
5.3	Payroll Personnel Workflows .....	33
5.3.1	Sponsorship of New Employee in Payroll Personnel .....	33
5.3.2	Sponsorship of Existing Employee in Payroll Personnel.....	35
5.3.3	Employee Information Change in Payroll Personnel.....	37
5.3.4	Employee Status Change in Payroll Personnel.....	38
5.3.5	Sponsorship Suspension in Payroll Personnel.....	39
5.3.6	Sponsorship Termination in Payroll Personnel.....	40
5.3.7	Sponsorship Reactivation in Payroll Personnel.....	42
5.3.8	Employee "Card Required" Change in Payroll Personnel .....	43
5.3.9	Employee Other Information Change in Payroll Personnel.....	45
5.4	Request Card Re-Issuance .....	46
5.4.1	Sponsorship Re-Issuance Process.....	47
<b>Section 6</b>	<b>Sponsorship Policies .....</b>	<b>49</b>
6.1	Sponsor Responsibilities.....	49
6.2	Sponsor Training .....	49
6.2.1	Resources for Initiating NACIs.....	49
6.2.2	Training for I.D. Validation .....	49
6.2.4	USACCESS Web Application Training .....	50
6.3	Identity Proofing .....	50
6.3.1	Disqualifying Information .....	51
6.3.2	ID Card Examination and Validation.....	51
6.3.3	IDs Applicants Are Required to Present for LincPasses .....	51
6.3.4	I.D. Validation Challenges .....	51
6.3.5	Altered SDL/OIDs .....	52



6.3.6	Counterfeit SDL/OIDs .....	52
6.3.7	Borrowed SDL/OIDs .....	53
6.3.8	I.D. Validation Resources .....	53
6.4	Background Investigations .....	54
6.5	Scheduling NACIs .....	56
<b>Section 7</b>	<b>Adjudication .....</b>	<b>59</b>
7.1	New Adjudication Record .....	60
7.2	Adjudication Workflows in EmpowHR .....	60
7.2.1	Fingerprint Adjudication in EmpowHR .....	60
7.2.2	Fingerprint Adjudication Appeals Process in EmpowHR .....	63
7.2.3	Background Investigation (BI) Process in EmpowHR .....	65
7.2.4	Background Investigation Appeals Process in EmpowHR .....	67
7.3	Adjudication Workflows in Payroll Personnel .....	69
7.3.1	Fingerprint Adjudication Process .....	69
7.3.2	Fingerprint Appeal Adjudication Process .....	71
7.3.3	Background Investigation Adjudication Process in Payroll Personnel .....	73
7.3.4	Background Investigation Appeals Adjudication Process in Payroll Personnel .....	75
<b>Section 8</b>	<b>Adjudication Policies .....</b>	<b>77</b>
8.1	Change to Adjudication Record Status .....	77
8.2	Adjudicator Responsibilities .....	77
8.3	Adjudicator Training .....	77
8.3.1	Verification of Contractor NACIs .....	78
8.3.2	Adjudication of NACI Records Checks .....	78
8.4	Adjudication of FBI Fingerprint Checks .....	80
8.5	Appeal Procedures for Denial or Revocation of Credential .....	80
8.5.1	Appeal Rights for Federal Service Applicants .....	80
8.5.2	Appeal Rights for Contractors and Affiliate Applicants .....	81
8.5.3	Record Retention .....	81
8.5.4	Use of Approved Forms .....	82
<b>Section 9</b>	<b>Enrollment Process .....</b>	<b>83</b>
9.1	New Enrollment .....	83
9.2	Invalid Source Documents .....	85
9.3	Incorrect Source Documents .....	85
<b>Section 10</b>	<b>Issuance .....</b>	<b>86</b>
10.1	Detailed Issuance Process .....	87
10.2	Invalid Card Printing Check .....	88
10.3	Wrong Cards Shipped to Valid Address .....	88
10.4	No Applicant Match for a Shipped Card .....	89
<b>Section 11</b>	<b>Activation .....</b>	<b>90</b>
11.1	Unattended Activation Workflow .....	90
11.1.1	Unattended Activation with Fingerprint Biometrics .....	90
11.1.2	Detailed Unattended Activation Process .....	91
11.2	Failed Unattended Activation .....	93
11.3	Attended Activation with Fingerprint Biometrics .....	93
11.4	Attended Activation Workflows .....	93
11.4.1	Detailed Attended Activation Process EmpowHR .....	93
11.4.2	Detailed Attended Activation Process Payroll Personnel .....	96
11.5	Failed Attended Activation .....	98
<b>Section 12</b>	<b>Security Officer .....</b>	<b>99</b>
12.1	Security Officer Security Event Processes .....	101
12.2	Security Officer Suspension Process .....	102
12.3	Security Officer Reactivation Process .....	103
12.4	Reissuance Process .....	105



<b>Section 13</b>	<b>Card Usage</b> .....	<b>107</b>
13.1	PIN Unlock .....	107
13.2	PIN Reset .....	108
13.3	Card Renewal.....	109
13.4	Attended Certificate Renewal.....	114
13.5	Unattended Certificate Renewal .....	115
<b>Appendix A</b>	<b>Acronyms</b> .....	<b>A-1</b>
<b>Appendix B</b>	<b>Sponsorship and Adjudication Forms</b> .....	<b>B-1</b>
<b>Appendix C</b>	<b>References</b> .....	<b>C-1</b>
<b>Appendix D</b>	<b>Data Preparation</b> .....	<b>D-1</b>

## List of Tables

Table 1: Document Organization.....	3
Table 2: Definitions.....	6

## List of Figures

Figure 1: Applicant process overview.....	8
Figure 2: Communication overview of applicant process.....	9
Figure 3: Sponsorship overview of the applicant process.....	9
Figure 4: Enrollment overview of the applicant process.....	10
Figure 5: Adjudication overview of the applicant process .....	10
Figure 6: Issuance overview of the applicant process.....	11
Figure 7: Activation overview of the applicant process .....	11
Figure 8: HSPD-12 PIV-II Process Overview EmpowHR (E0).....	12
Figure 9: HSPD-12 PIV-II Process Overview Payroll Personnel (P0).....	13
Figure 10: Role Administrator Overview.....	14
Figure 11: Role Administrator (1) .....	15
Figure 12: Sponsorship Overview .....	17
Figure 13: LincPass Distribution Risk Assessment.....	18
Figure 14: Sponsorship of New Employee in EmpowHR (2E-1a).....	19
Figure 15: Sponsorship of Existing Employee in EmpowHR (2E-1b) .....	21
Figure 16: Employee Information Change in EmpowHR (2E-2) .....	23
Figure 17: Employment Status Change in EmpowHR(2E-2a) .....	24
Figure 18: Sponsorship Suspension EmpowHR (2E-2a.1) .....	25
Figure 19: Sponsorship Termination in EmpowHR (2E-2a.2).....	26
Figure 20: Sponsorship Reactivation in EmpowHR (2E-2a) .....	28
Figure 21: Sponsorship Card Required Change Process (2E-2b).....	29
Figure 22: Sponsorship Employee Other Information Change in EmpowHR (2E-2c) .....	31
Figure 23: Sponsorship of New Employee in Payroll Personnel (2P-1a).....	33
Figure 24: Sponsorship of Existing Employee in Payroll Personnel (2P-1b) .....	35
Figure 25: Sponsorship Employee Information Change in Payroll Personnel (2P-2) .....	37
Figure 26: Sponsorship Employee Status Change in Payroll Personnel (2P-2a).....	38
Figure 27: Sponsorship Suspension in Payroll Personnel (2P-2a.1) .....	39
Figure 28: Sponsorship Termination in Payroll Personnel (2P-2a.2).....	40
Figure 29: Sponsorship Reactivation in Payroll Personnel (2P-2a.3) .....	42
Figure 30: Sponsorship Employee "Card Required" Change in Payroll Personnel (2P-2b) .....	43
Figure 31: Employee Other Information Change in Payroll Personnel (2P-2c) .....	45
Figure 32: Sponsorship Re-Issuance (2EP-3).....	47
Figure 33: Adjudication Overview.....	59
Figure 34: Fingerprint Adjudication in EmpowHR (3E-1) .....	61
Figure 35: Fingerprint Appeal Process in EmpowHR (3E-1a).....	63
Figure 36: Background Investigation in EmpowHR (3E-2).....	65



Figure 37: Background Investigation Appeals Process in EmpowHR (3E-2a) ..... 67  
Figure 38: Fingerprint Adjudication in Payroll Personnel (3P-1) ..... 69  
Figure 39: Fingerprint Appeal Adjudication Process in Payroll Personnel (3P-1a)..... 71  
Figure 40: Background Investigation Adjudication Process in Payroll Personnel (3P-2)..... 73  
Figure 41: Background Investigation Appeals Adjudication Process (3P-2a)..... 75  
Figure 42: Enrollment Overview ..... 83  
Figure 43: Enrollment (4)..... 84  
Figure 44: Issuance Overview..... 86  
Figure 45: Detailed Issuance Process (5) ..... 87  
Figure 46: Activation Overview..... 90  
Figure 47: Unattended Activation (6-1) ..... 91  
Figure 48: Attended Activation (6E-1a) ..... 94  
Figure 49: Detailed Attended Activation in Payroll Personnel (6P-1a)..... 96  
Figure 50: Security Officer Overview..... 99  
Figure 51: Security Officer Process (7) ..... 101  
Figure 52: Security Officer Suspension (7-1) ..... 102  
Figure 53: Security Officer Reactivation (7-2) ..... 103  
Figure 54: Security Officer Re-issuance in Payroll Personnel (7-3)..... 105  
Figure 55: Card Usage-Pin Unlock (8-1) ..... 107  
Figure 56: Card Usage-Pin Reset (8-2)..... 108  
Figure 57: EmpowHR Card Renewal Process (8E-3) ..... 110  
Figure 58: Card Renewal in Payroll Personnel (8P-3) ..... 112  
Figure 59: Attended Certificate Renewal (8-4) ..... 114  
Figure 60: Unattended Certificate Renewal (8-5)..... 115

DRAFT



## Section 1 Executive Summary

This document presents a set of business processes and policies for implementation of PIV-II compliant credentials to USDA Employees. 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 to 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 the 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. USDA has named their PIV-II compliant ID card the LincPass, as it is designed to link a person's identity to an ID card and the card to a person's ability to physically and logically access federally controlled buildings and information systems, respectively.

USDA is one of the major Departments participating in General Services Administration (GSA) Shared Services solution called the USAccess Program. GSA has provided basic processes and procedures for each credential issuing process phase: Sponsorship, Adjudication, Enrollment, Issuance, and Activation. Some parts of these processes require agency-specific policies. USDA has tailored the basic GSA processes for implementation for Enrollment, Issuance and Activation to work within USDA constructs. USDA Sponsorship and Adjudication policies and procedures have been included in more detail in this document to comply with the HSPD-12 directive.

A planned rollout of LincPasses to USDA employees, contractors, and affiliates will be implemented by organization and geographic location. This document covers the business processes and procedures for credentialing only USDA employees. Credentialing for contractors and affiliates will be covered in another document.

## Section 2 Introduction

### 2.1 Background

HSPD-12 was issued on August 27, 2004 and requires “a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)”. All Federal Agencies must implement HSPD-12 in accordance with the process and technical standards laid out in the National Institute of Standards and Technology (NIST) Federal Information Processing Standard 201-1 (FIPS 201-1) and Office of Management and Budget (OMB) guidance.

There are two major sections in FIPS 201-1. Part One describes the minimum requirements for a Federal Personal Identity Verification (PIV-I) system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance. PIV-I is intended to ensure the integrity of the process for verifying the identity of employees and contractors who are issued an ID card. FIPS 201-1, Part Two (PIV-II) provides the technical specifications for the new ID “smart” card and federal agency PIV systems so that they are interoperable.

### 2.2 Document Organization

This document is organized in the following sections:

Section No.	Title	Description
1	Executive Summary	A summary of the purpose of this document
2	Introduction	This section contains the background, purpose, document organization, and considerations for the business process review
3	PIV-II Overview	A high-level overview of the PIV-II credentialing process for an Employee, as well as an overview of the workflows for the credentialing process for agencies using EmpowHR and Payroll Personnel
4	Role Administrator	Description of the role and responsibilities of the Role Administrator
5	Sponsorship	Workflows for sponsorship
6	Sponsorship Policies	Sponsor’s role and responsibilities, and sponsorship policies
7	Adjudication	Workflows for adjudication

Section No.	Title	Description
8	Adjudication Policies	Adjudicator's role and responsibilities, and adjudication policies
9	Enrollment Process	Workflows for enrollment process
10	Issuance	Workflows for issuance process
11	Activation	Workflows for activation process
12	Security Officer	Security Officer roles, responsibilities, and workflows
13	Card Usage	Workflows for maintenance activities of the LincPass
Appendix A	Acronyms	A list of all acronyms utilized in the workflow analysis
Appendix B	Sponsorship and Adjudication Forms	Basic forms used by sponsors and adjudicators
Appendix C	References	A table listing and describing the documentation that was reviewed to develop this document
Appendix D	Data Preparation	Placeholder for instruction checklists for data cleanup for the Agencies

*Table 1: Document Organization*

### 2.3 Definitions

Term	Description
Applicant	The Applicant is an individual requesting a credential from an agency that is a participant in the USAccess system . The Applicant may be a current or prospective Federal hire, a Federal employee, or a contractor.
Adjudicator	A Government Employee of the sponsoring agency who resolves any issues or failures of the background check process and authorizes or denies the printing of a PIV card.
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.
Credential	Evidence attesting to one's right to credit or authority; in this standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.
Enrollment Process	The process of identity-proofing and capturing the applicant's identification information, identity source documents, and biometrics.



Term	Description
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.
HSPD-12	Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," dated August 27, 2004
Issuer/Activator	The Issuer/Activator is the individual responsible for processing card 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.
Identity Management System (IDMS)	One or more systems or applications that manage the identity verification, validation, and card issuance process. The IDMS software is used by PIV Registrars to enroll Applicants.
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.
Logical Access Control System (LACS)	Protection mechanisms that limit users' access to information technology (IT) systems by restricting their form of access to those systems necessary to perform their job function. These LACS may be built into an operating system, application, or an added system.
National Agency Check with Inquiries (NACI)	The basic and minimum investigation required of all Federal employees and contractors consisting of searches of the OPM Security/ Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (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).
U.S. Office of Personnel Management (OPM)	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.
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.



Personal Identity Verification II (PIV-II)  
Business Processes, Policies, and Procedures for  
Employees

Version 1.1

Term	Description
Physical Access Control System (PACS)	Protection mechanisms that limit users' access to physical facilities or areas within a facility necessary to perform their job function. 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).
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.
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.
Registrar	An individual responsible for the identity proofing the applicant, as well as capturing biographic and demographic information, a digital photo, and biometrics.
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 roles policies are followed and will verify that all the training certification requirements have been met.
Enrollment Role Administrators	Role Administrators for Enrollment can be identified to facilitate the role of the Registrar for USDA leased stations or when GSA stops providing Registrars to USDA. Enrollment Role Administrators will identify Registrars needed for Enrollment stations if they are hosting an Enrollment within their Agency facilities.
USDA Role Administrator	USDA Role Administrator assigns Agency Role Administrator, Security Officer, Sponsor, Registrar, Adjudicator, and Activator roles within USDA.
Security Role Administrators	Role Administrators for Security designate the role of Security Officer to the appropriate individuals who meet the position guidelines and facilitate and monitor the responsibilities of the Security Officer. They decide how many Security Officers are needed in their Agency.
Sponsor/Adjudicator Role Administrators	Role Administrators for Sponsors/Adjudicators identify Sponsors and Adjudicators within their agency and facilitate the training, credentialing, and responsibilities of the Sponsors and Adjudicators.
Sponsor	The individual who substantiates the need for a PIV credential to be issued to an applicant, enters the applicant's required sponsorship data elements into the system, and remains aware of the applicant's status and continuing need for holding a PIV credential.



Term	Description
Security Officer	Security Officer is the individual responsible for maintaining credential security as well as physical building security for their agency.
Standard Form (SF)-85	Questionnaire for Non-Sensitive Positions
Standard Form (SF)-85P	Questionnaire for Public Trust Positions
Standard Form (SF)-86	Questionnaire for National Security Positions
Standard Form (SF)-87	Fingerprint Chart used to conduct FBI fingerprint checks for federal appointees and employees and applicants for federal employment

Table 2: Definitions

DRAFT

## **Section 3 PIV-II Process Overview**

### **3.1 *Applicant Process***

The following diagram displays an overview of processing a new applicant (new employee) for a PIV-II compliant card (LincPass). In this case, it is assumed the applicant does not have a previous background investigation on file. Each process is presented in more detail in separate sections.

DRAFT

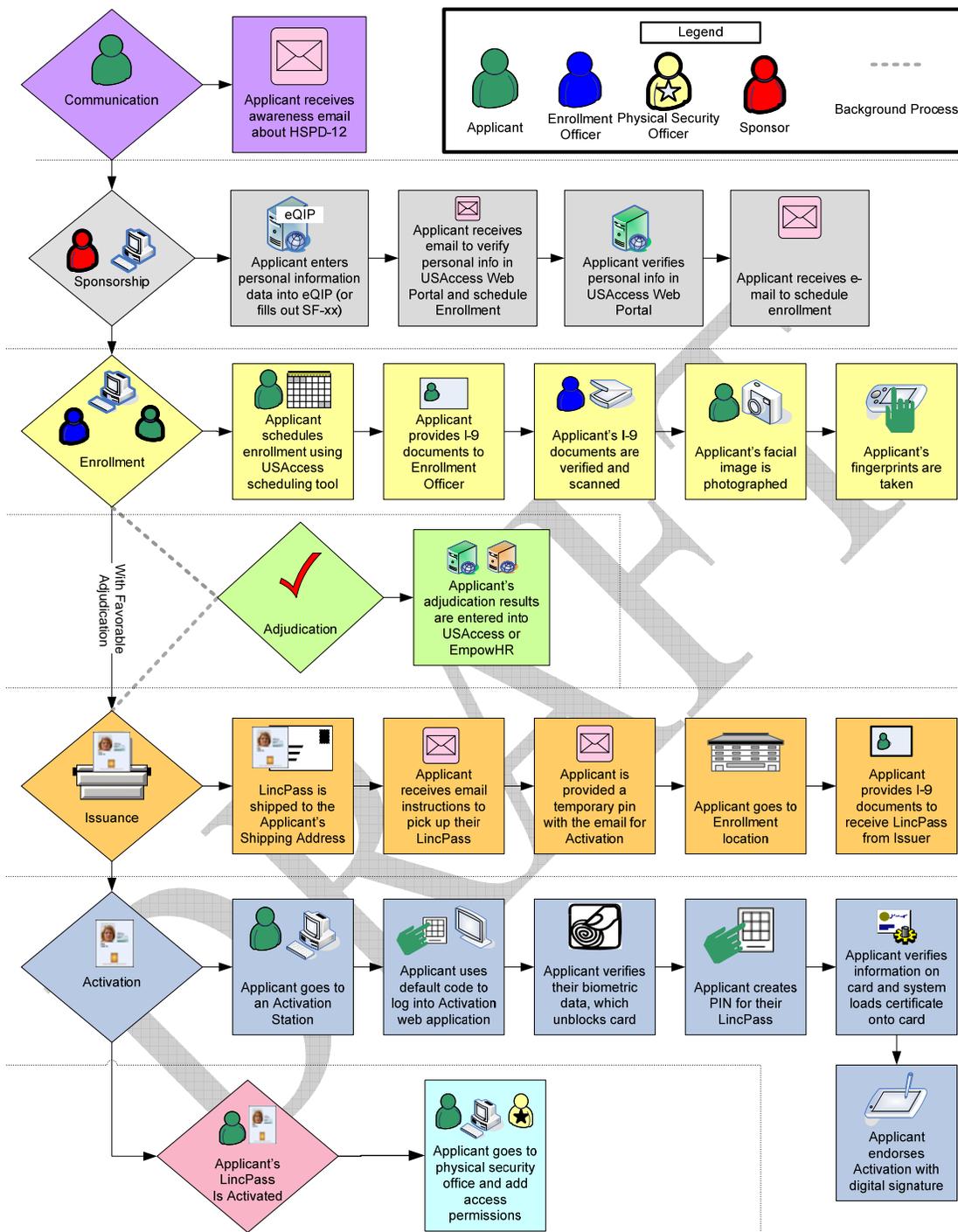


Figure 1: Applicant process overview

### 3.1.1 PART I: Communication

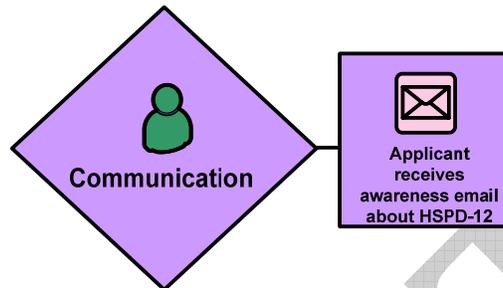


Figure 2: Communication overview of applicant process

The first step in the overall process is for the Applicant to receive an awareness email from the HSPD-12 Implementation Team about the HSPD-12 directive. This email gives the Applicant information about what HSPD-12 is along with general information about what will be required of the Applicant in order to comply with HSPD-12.

### 3.1.2 PART II: Sponsorship

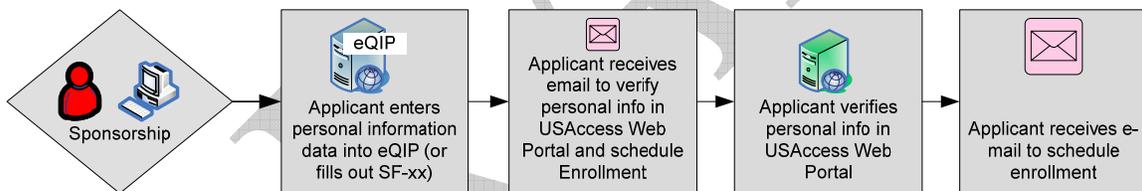


Figure 3: Sponsorship overview of the applicant process

In Sponsorship, the Applicant's need for a LincPass is substantiated and their initial information is entered into the appropriate (e.g. EmpowHR, Payroll Personnel and USAccess) system by a Sponsor.

1. Sponsorship begins with the submission of background information into a USDA accepted background investigation process.
2. The Applicant's Sponsorship information is sent to the USAccess System.
3. The USAccess System then emails the Applicant asking them to verify their information in the system via the USAccess Web Portal.
4. The applicant is notified that he/she must schedule an appointment at an enrollment station. The applicant is directed to a Web-based scheduling tool to locate an enrollment station and schedule the appointment.

### 3.1.3 PART III: Enrollment

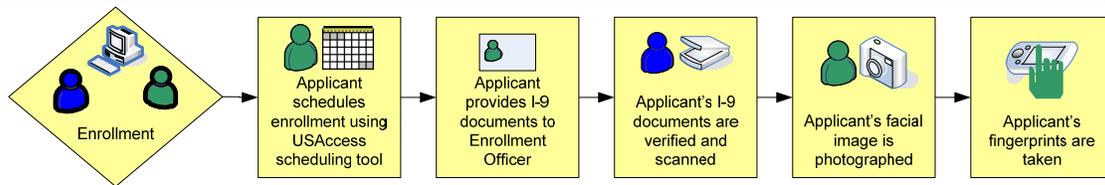


Figure 4: Enrollment overview of the applicant process

In the Enrollment step, the Applicant's identity documentation is verified and their biometric information is captured in the system.

1. After scheduling an Enrollment appointment, the Applicant goes to an Enrollment station.
2. The Applicant provides the Registrar their I-9 documents.
3. The Registrar verifies and scans the documents into the system.
4. The Applicant's facial image is captured in the system via a digital photograph.
5. The Applicant's fingerprints are taken and captured in the USAccess system.
6. The scanned documents, photo, and fingerprints are in Applicant's record.

### 3.1.4 PART IV: Adjudication

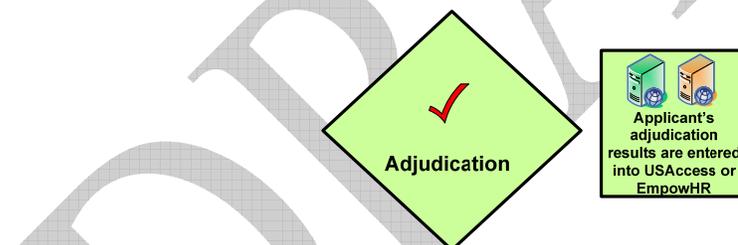


Figure 5: Adjudication overview of the applicant process

During this step, the results of the Applicant's background check are received and evaluated.

1. For Applicants in EmpowHR, the Adjudication results are automatically sent to the USAccess System. For those in Payroll Personnel, the Adjudicator must manually input the results into the USAccess System.
2. If the Applicant's background investigation was favorably adjudicated the process moves on to Issuance.

### 3.1.5 PART V: Issuance

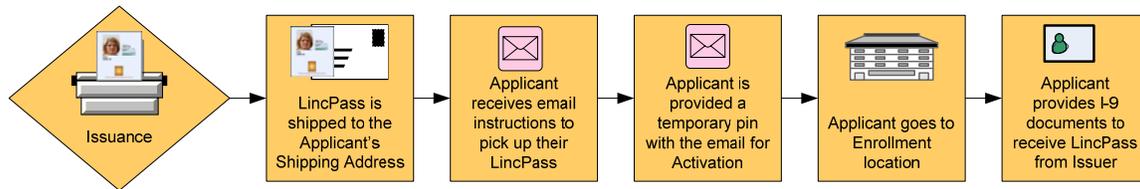


Figure 6: Issuance overview of the applicant process

In the Issuance process, the Applicant physically acquires their LincPass.

1. The LincPass is produced, printed, and electronically locked, then shipped to the address provided as the Shipping Address in the USAccess System.
2. The Applicant receives email instructions from the USAccess System about how to pick up their LincPass along with a temporary activation PIN.
3. The Applicant goes to the Sponsor-specified address to get their LincPass.
4. The Applicant provides their I-9 documents for identity verification to the issuing official in order to obtain their LincPass.

### 3.1.6 PART VI: Activation

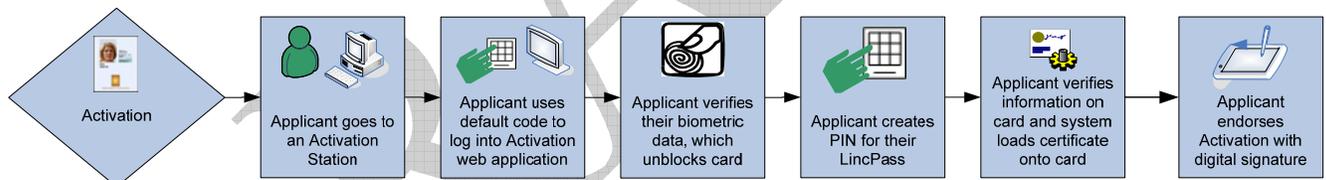


Figure 7: Activation overview of the applicant process

In the Activation process, the LincPass is “activated” so that it can be used by the Applicant.

1. Applicant takes the LincPass to an Activation station.
2. The Applicant uses the temporary PIN provided to log into the Activation application.
3. The Applicant is verified via their biometric information; the card is then unlocked.
4. The Applicant creates a new PIN for their LincPass.
5. The Applicant verifies their information on the card; the system then loads the certificates onto the card.
6. The Applicant endorses the activation with a digital signature.
7. The LincPass is now fully activated and ready to use.

### 3.2 HSPD-12 PIV-II Process Overview in EmpowHR

The following diagram details the overview of the PIV-II process in EmpowHR to include Sponsorship, Adjudication, Enrollment, Issuance, Activation, and use cases.

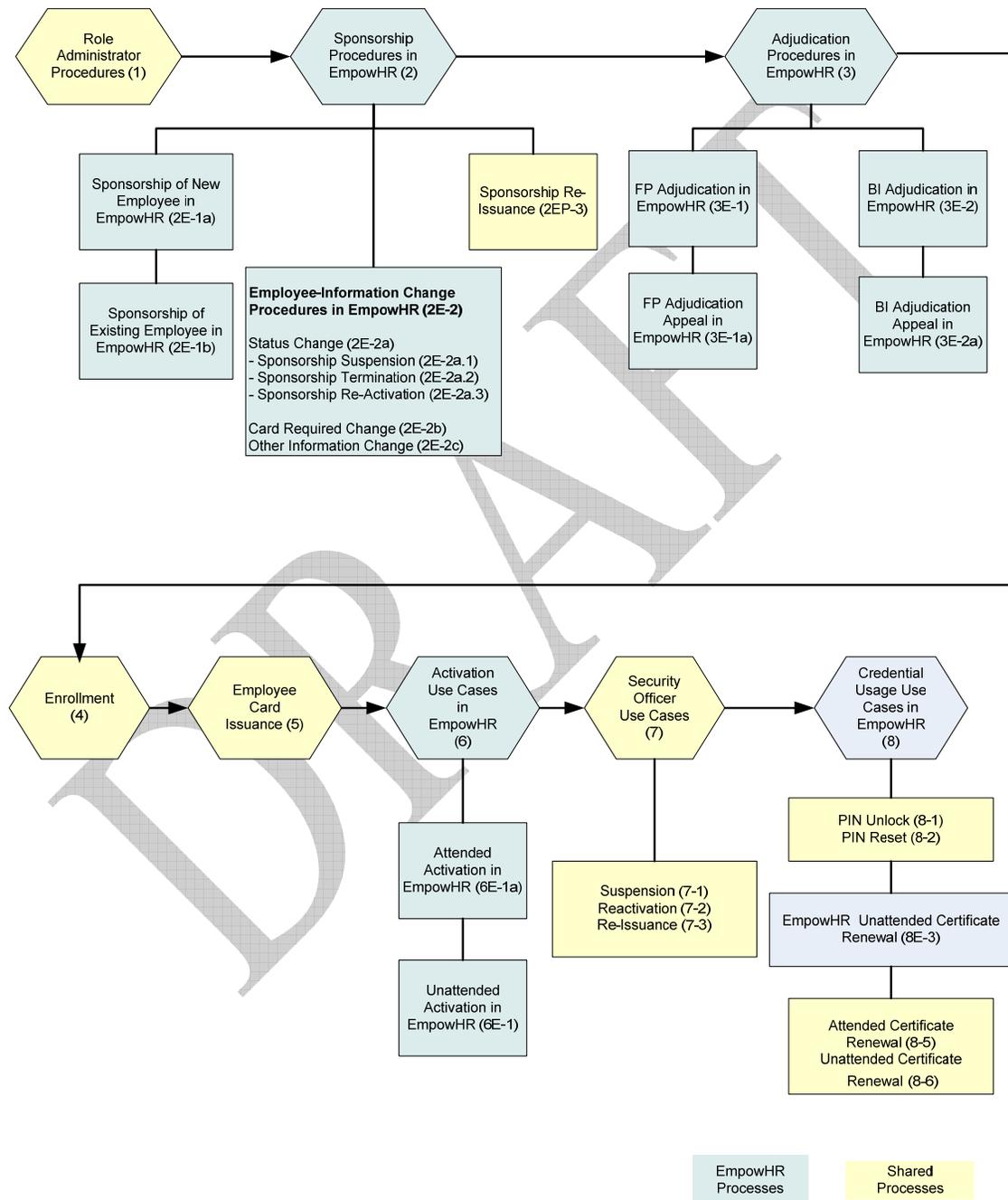


Figure 8: HSPD-12 PIV-II Process Overview EmpowHR (E0)

### 3.3 HSPD-12 PIV-II Process Overview in Payroll Personnel

The following diagram details the overview of the PIV-II process in Payroll Personnel to include Sponsorship, Adjudication, Enrollment, Issuance, Activation, and etc.

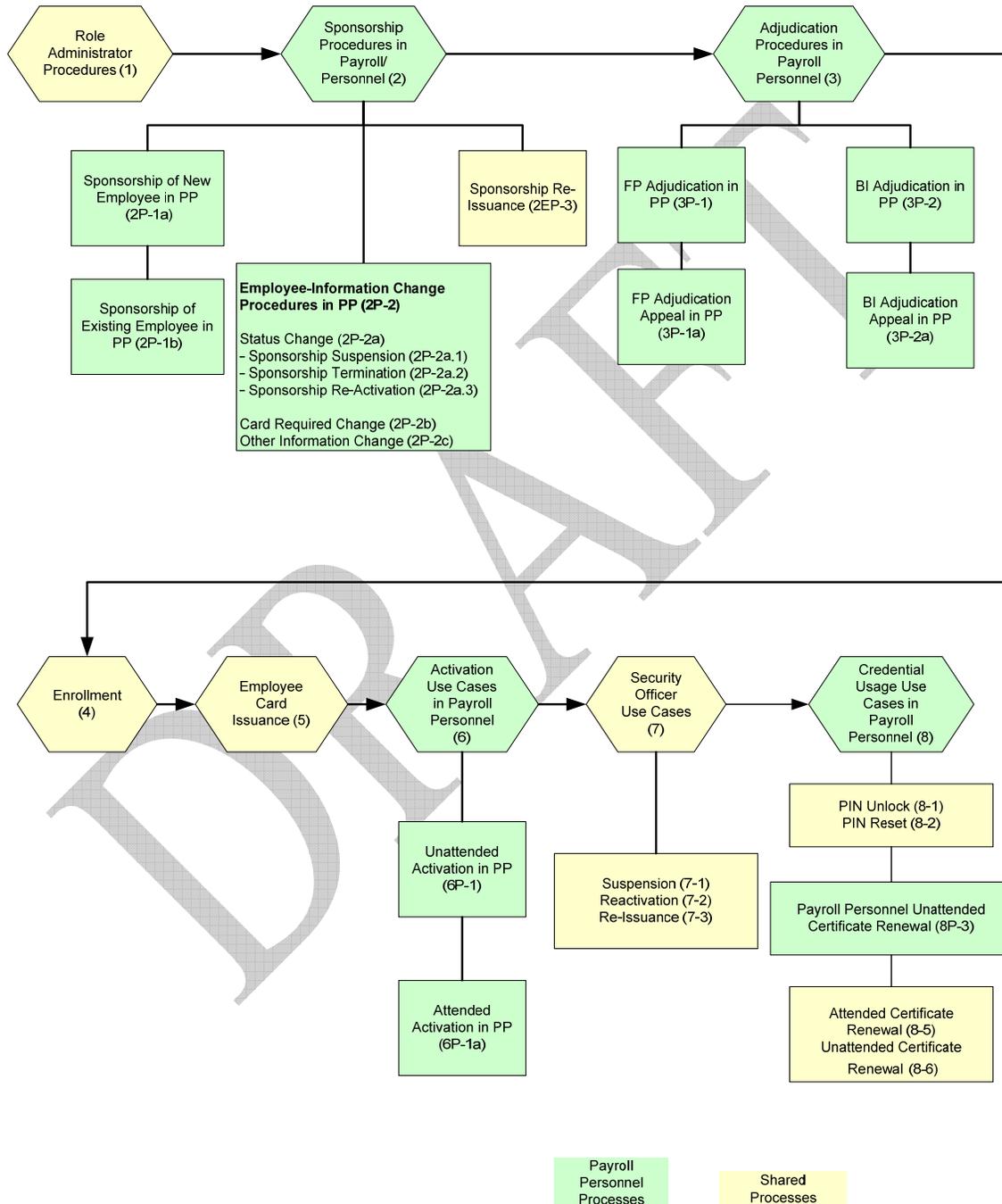


Figure 9: HSPD-12 PIV-II Process Overview Payroll Personnel (P0)

## Section 4 Role Administrator



Figure 10: Role Administrator Overview

FIPS 201-1 discusses the role of an Approval Authority who “establishes organizational chain of command within the Identity Management System (IDMS) for PIV application approvals. The Approval Authority will manage the total scope of the chain of trust established in functional processes, as well as appropriate privacy and security controls.” The USAccess Program and USDA calls this approval authority the Role Administrator. The Role Administrator must have training, be certified, and be issued a LincPass before beginning HSPD-12 responsibilities.

### LincPass Hierarchy

The USDA Role Administrator takes priority over the Sponsors and Adjudicators to receive a LincPass. Once the USDA Role Administrator obtains a LincPass, he/she can assign an Agency Role Administrator, Security Officer, Sponsor, Adjudication, Activator/Issuer and Registrar roles within USDA. The number of roles identified within an agency is up to the discretion of the Agency Role Administrator, depending upon the number of employees and geographic location of employees.

The USDA Role Administrator must first identify the Role Administrator for each of the Agencies. Once the Agency Role Administrators are identified, trained, and credentialed, they can designate other Agency Role Administrators within their agency to further disseminate the roles and responsibilities. These Agency Role Administrators can concentrate on the type of roles they will be identifying within their agency. The Agency Role Administrator verifies that the appropriate separation of roles policy is followed and that all training certification requirements have been met prior to delegating role administration. Also, if any roles overlap, the Role Administrator is required to determine the impact of assigning the new role to an individual.

### Role Administrator--Security

The Role Administrator--Security designates the role of the Security Officer to the appropriate individuals who meet the position guidelines. The Role Administrator--Security will facilitate and monitor the responsibilities of the Security Officer. They will decide how many Security Officers are needed in their Agency. The Security Officers will have the ability to suspend an employee’s LincPass through the USAccess Web Portal or EmpowHR when there is a security related situation. The Agency Security Officer can only access records only for his/her designated agency. The Security Officer will investigate the situation with the Role Administrator Sponsor and resolve the issue.

**Role Administrator--Sponsor/Adjudicator**

The Role Administrator--Sponsor/Adjudicator will identify Sponsors and Adjudicators within his/her agency. In addition to identifying the number of Sponsors and Adjudicators needed in the agency, the Role Administrator--Sponsor/Adjudicator will facilitate the Sponsor/Adjudicator's training, credentialing, and will oversee the Sponsor/Adjudicator's HSPD-12 activities.

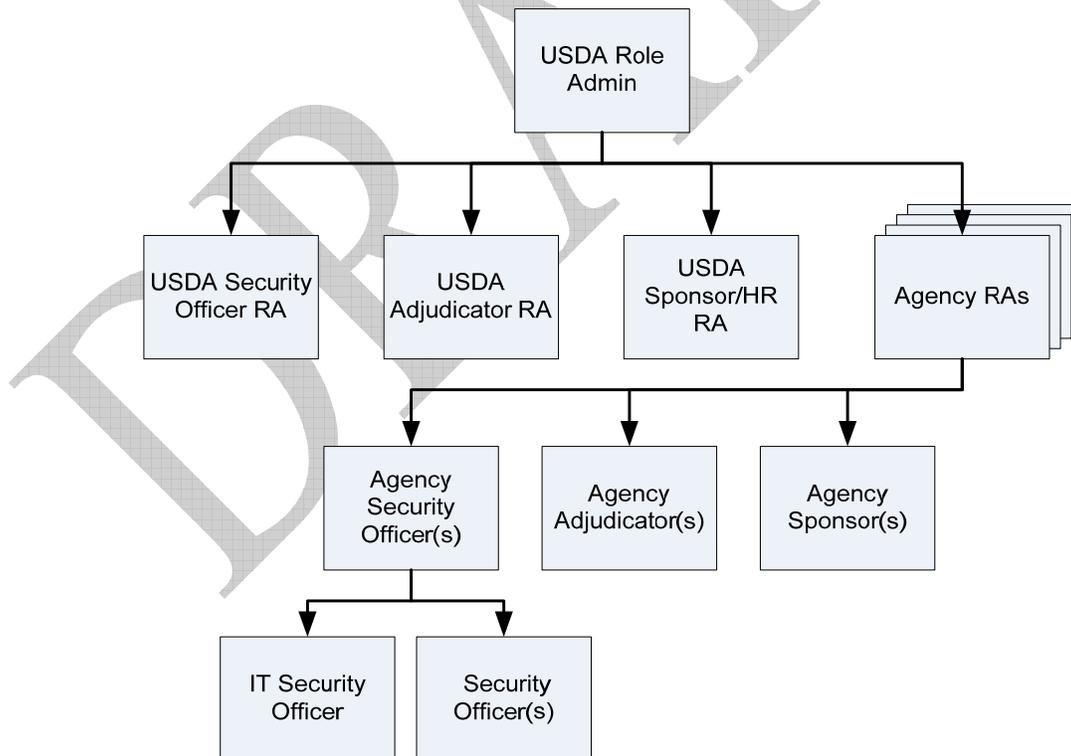
**Role Administrator--Enrollment**

An Enrollment Role Administrator may be identified to facilitate the role of the Registrar for USDA leased stations or when GSA stops providing Registrars to USDA. Enrollment Role Administrators will identify Registrars needed for Enrollment stations if they are hosting an Enrollment within their Agency facilities.

All designated Agency Role Administrators will report to the lead Agency Role Administrator.

**4.1 Role Administrator**

The following diagram details the relationships and workflows from the top level USDA Role Administrator down to the individual Sponsors, Adjudicators, etc.



1

Figure 11: Role Administrator (1)



1. The USDA Role Administrator receives training, is certified, and is issued a LincPass.
2. If necessary, the USDA Role Administrator can designate additional USDA Role Administrators with the same privileges.
3. The USDA Role Administrator designates Agency Role Administrators (ARAs).
4. The ARA(s) receive training, certification, and a LincPass.
5. The ARA(s) can designate additional ARAs for their Agency if necessary. Additionally, it may be beneficial to split designations of ARAs to specific process roles (i.e. A Security Officer ARA who is in charge of designating Security Officers for the Agency or a Sponsor ARA who is in charge of designating the Sponsors for the Agency, etc.)
6. The ARA(s) designate the Security Officer, Registrar, Adjudicator, and Sponsor for their Agency. The ARA can designate as many of each as is necessary for their Agency.
7. The Security Officer(s), Registrar(s), Adjudicator(s), and Sponsor(s) receive training, certification, and LincPasses.

DRAFT

## Section 5 Sponsorship

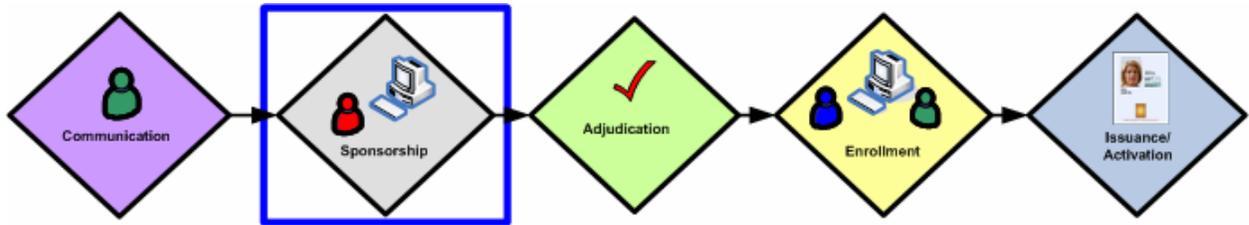


Figure 12: Sponsorship Overview

The issuing of PIV-II credentials begins with an authorized individual sponsoring an Applicant. This individual is called the Sponsor. Sponsors are individuals who act on behalf of the Department to request LincPass credentials for USDA Applicants (employees, contractors, or affiliates). Depending on the Applicant’s employment status, a Sponsor may be a federal supervisor, contracting officer, contracting officer’s representative, or other federal official. The Sponsor must have training and a LincPass in order to perform HSPD-12 Sponsor functions.

The Sponsorship process ensures that only individuals with a valid need for a credential are issued a LincPass. Sponsorship is an inherent governmental function where an authorized Federal Employee enters a person’s identity record into the system and approves it for enrollment. All Sponsors are required to enroll and obtain a LincPass prior to conducting any Sponsor responsibilities, and must complete Sponsor training.

Each agency Sponsor will need to determine who receives a LincPass. The LincPass Distribution Risk Assessment provides guidance on how to determine this. The first tier asks “Does the applicant access a level 2 or greater internal eAuthentication account or other protected resources or have a USDA email account?” If yes, the applicant requires a LincPass. The second tier asks “Does the applicant have access to sensitive information? If yes, the applicant requires a LincPass. The third question asks if the applicant requires unescorted access in mission critical or National Capital Region areas or as an individual agency determines as a secure facility. If yes, the applicant requires a LincPass. If no, the applicant receives a site or visitor badge based on the agency’s local risk assessment requirements.

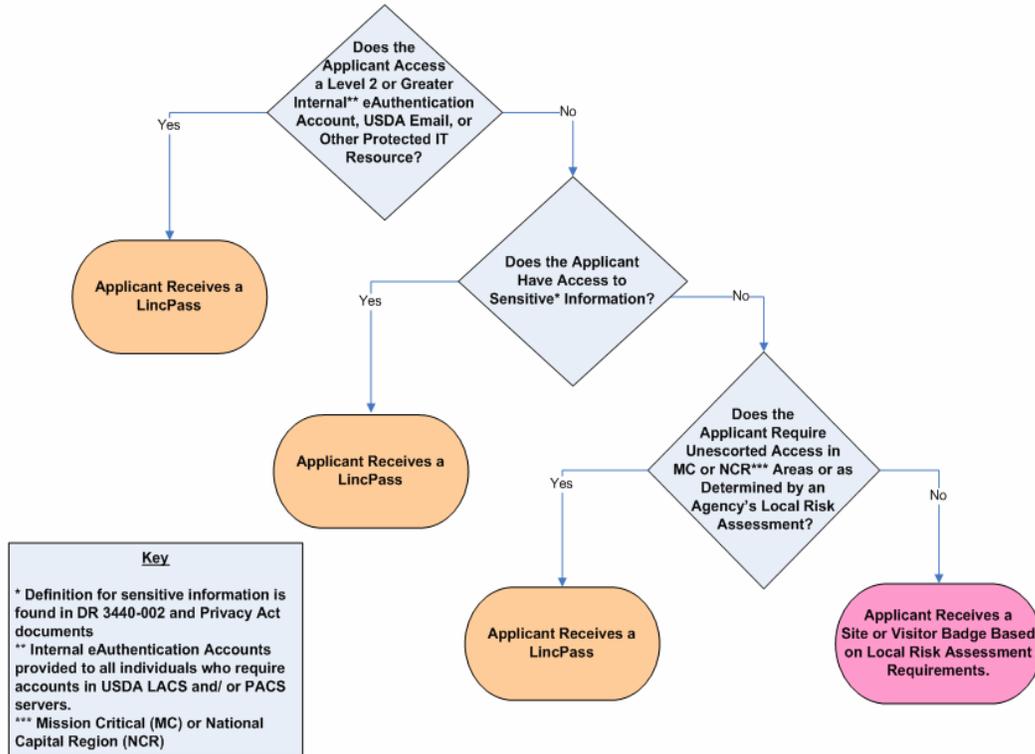


Figure 13: LincPass Distribution Risk Assessment

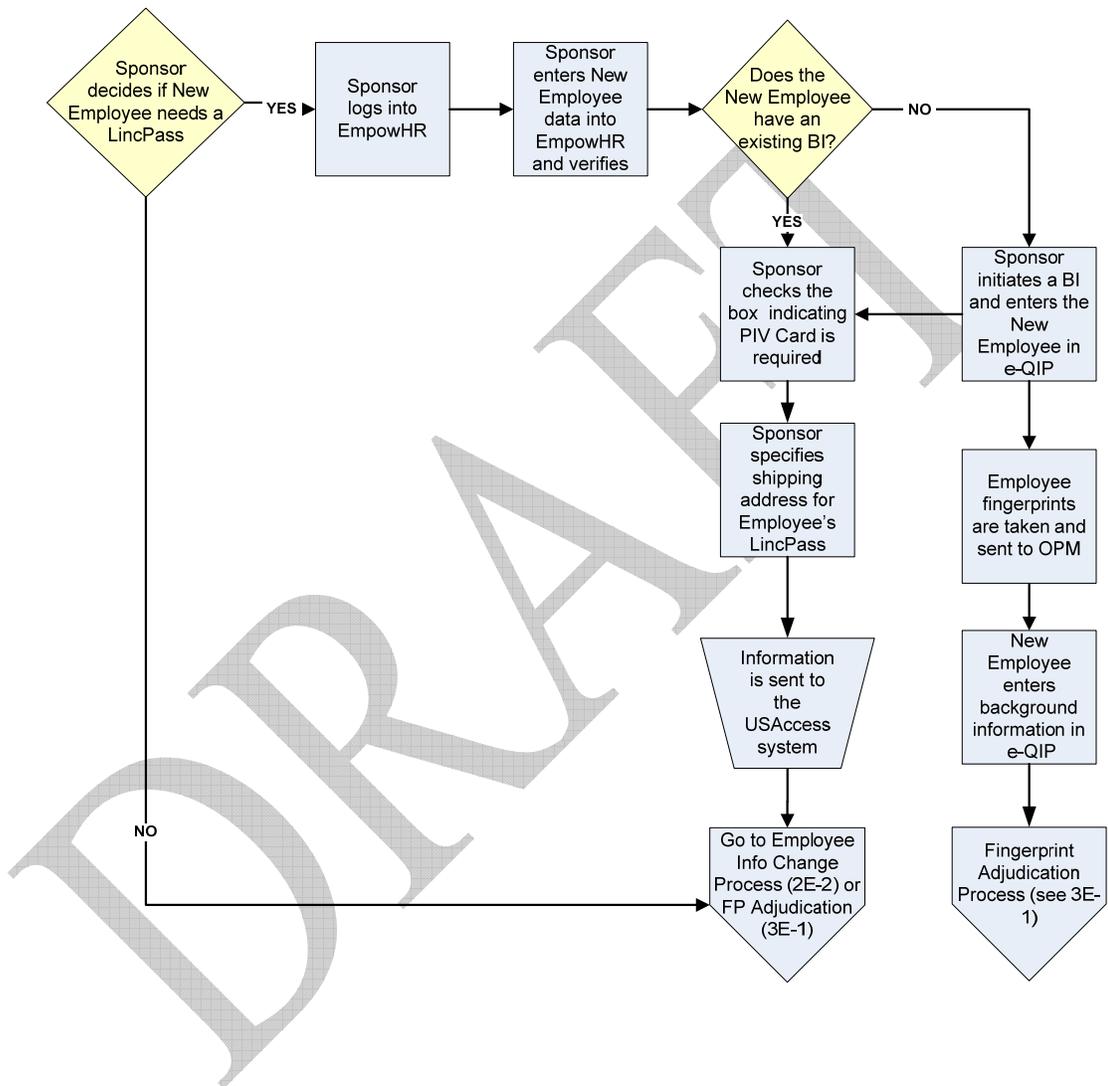
## 5.1 Overview of Sponsorship of Employees

For USDA employees the Sponsor can be Human Resource personnel, the employee's supervisor, or a Program Official. Sponsors must take training and be certified as Sponsors before beginning HSPD-12 responsibilities. Sponsors use the Risk Assessment to determine whether the Applicant requires a LincPass. A Sponsor initiates a background investigation and enter Applicant in e-QIP (or initiate background investigation paperwork if e-QIP is not available). Applicants enter background information in e-QIP for investigation (or fills out paperwork).

## 5.2 EmpowHR Workflows

### 5.2.1 First Time Sponsorship of New Employee in EmpowHR

The following diagram details the workflow of the first-time sponsorship of a new employee in the EmpowHR system.



2E-1a

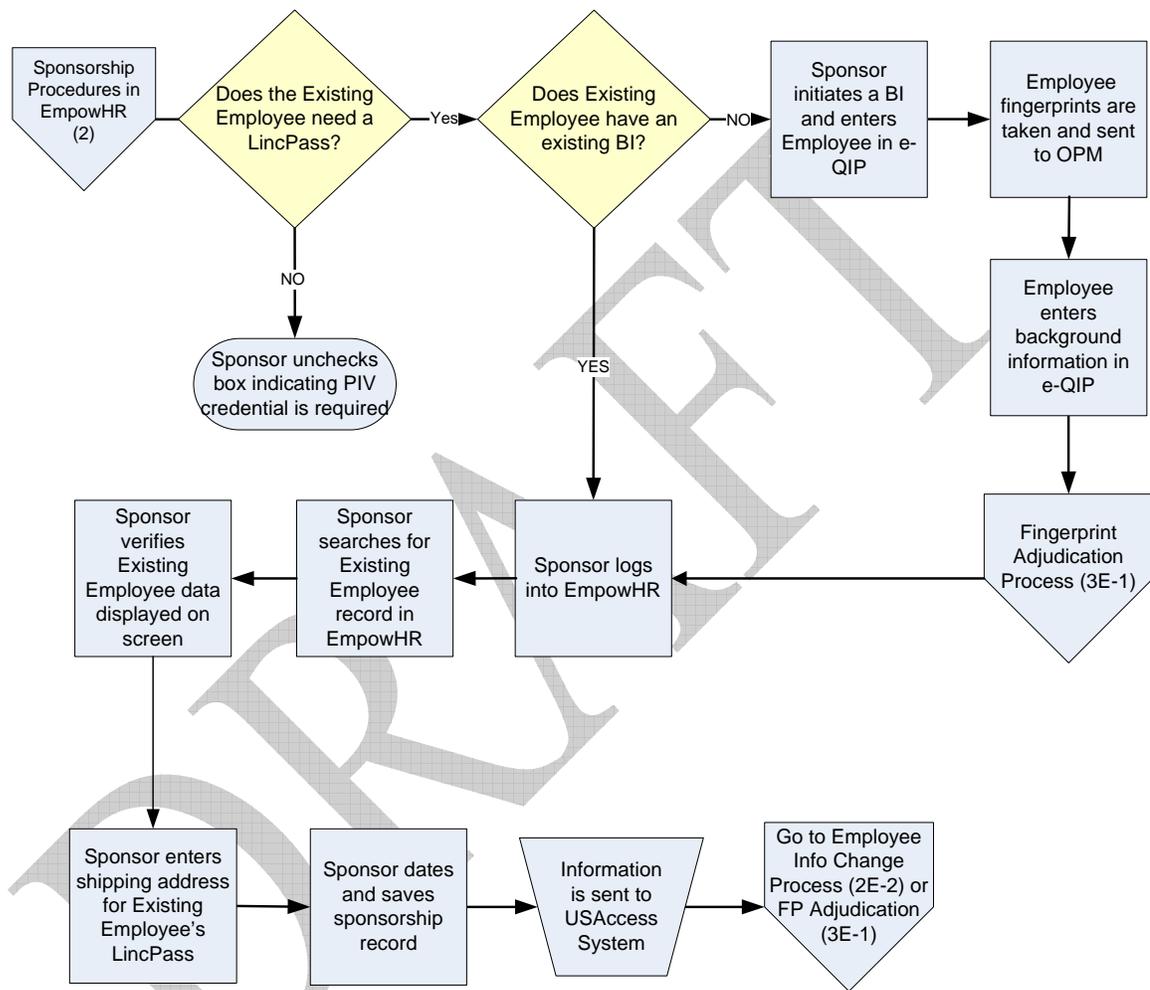
Figure 14: Sponsorship of New Employee in EmpowHR (2E-1a)

1. Sponsor determines if the Employee needs a LincPass using the LincPass Distribution Risk Assessment.

2. Sponsor logs into EmpowHR.
3. Sponsor enters the Employee's information into EmpowHR and then verifies that all information is correct.
4. If the Employee does not have an existing BI, the Sponsor initiates one by entering the Employee's information in e-QIP if accessible. If not accessible, the Sponsor uses the SF-85, SF-85P, or SF-86 paper form to initiate the BI.
  - a. The Employee's fingerprints are captured and sent to OPM for the fingerprint check.
  - b. The Employee then goes into e-QIP, if accessible to enter their information; otherwise they enter the information on the SF-85, 85P or 86 paper form.
  - c. The Sponsorship process will move on while the Fingerprint Check is in progress (results will be evaluated during Adjudication [3E-1]).
5. The Sponsor checks the box indicating that a PIV card is required.
6. Sponsor provides the Employee's shipping address
7. Sponsor saves the EmpowHR employee record and the date is captured
8. Employee record is sent to the USAccess System.
9. Sponsor goes to the Employee Information Change Process (2E-2) if the Employee's Information or Status changes; otherwise go to the Fingerprint Adjudication Process (3E-1).

### 5.2.2 First-Time Sponsorship of Existing Employee in EmpowHR

The following diagram details the workflow of the sponsorship of an existing employee in the EmpowHR system.



**2E-1b**

Figure 15: Sponsorship of Existing Employee in EmpowHR (2E-1b)

1. If the Employee does not have an existing BI, the Sponsor initiates one by entering the Employee's information in e-QIP if accessible. If not accessible, the Sponsor uses the SF-85, 85P, or 86 paper form to initiate the BI.
  - a. The Employee's fingerprints are captured and sent to OPM for the fingerprint check.
  - b. The Employee then goes into e-QIP, if accessible to enter their information; otherwise they enter the information on the SF-85, 85P, or 86 paper form.
  - c. The sponsorship process will move on while the fingerprint check is in progress (results will be evaluated during Adjudication (3E-1)).
2. If a LincPass is not needed, the Sponsor unchecks box indicating that a PIV card is not required.
3. The Sponsor logs into EmpowHR and searches for the Employee's record.
4. The record is found and the Sponsor views and verifies that all the Employee information is correct.
5. If LincPass is needed, Sponsor provides the Employee's shipping address.
6. Sponsor saves the EmpowHR Employee record and the date is captured.
7. Employee record is sent to the USAccess System.
8. Sponsor goes to the Employee Information Change Process (2E-2) if the Employee's Information or Status changes; otherwise go to the Fingerprint Adjudication Process (3E-1).

### 5.2.3 Employee Information Change in EmpowHR

The following diagram details the workflow of information change of an existing employee in the EmpowHR system

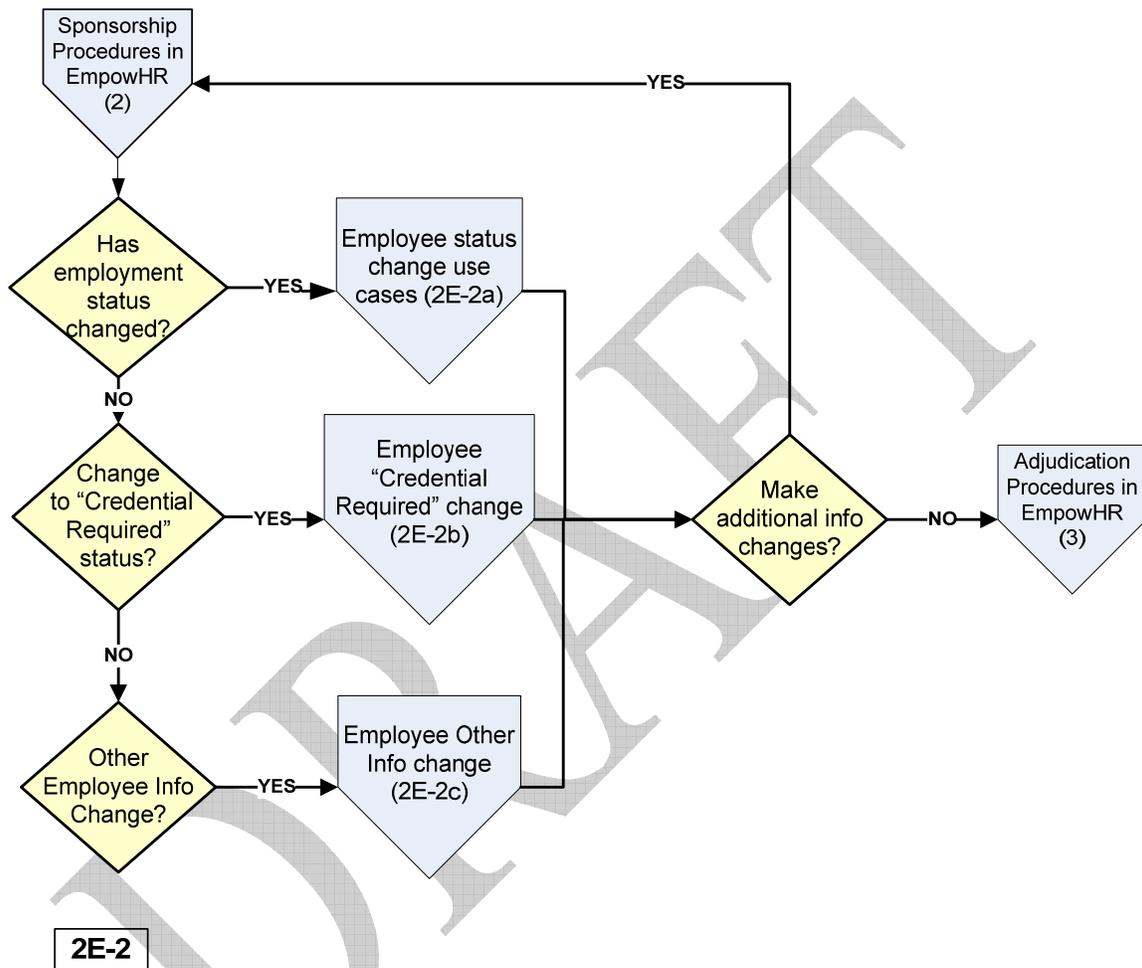
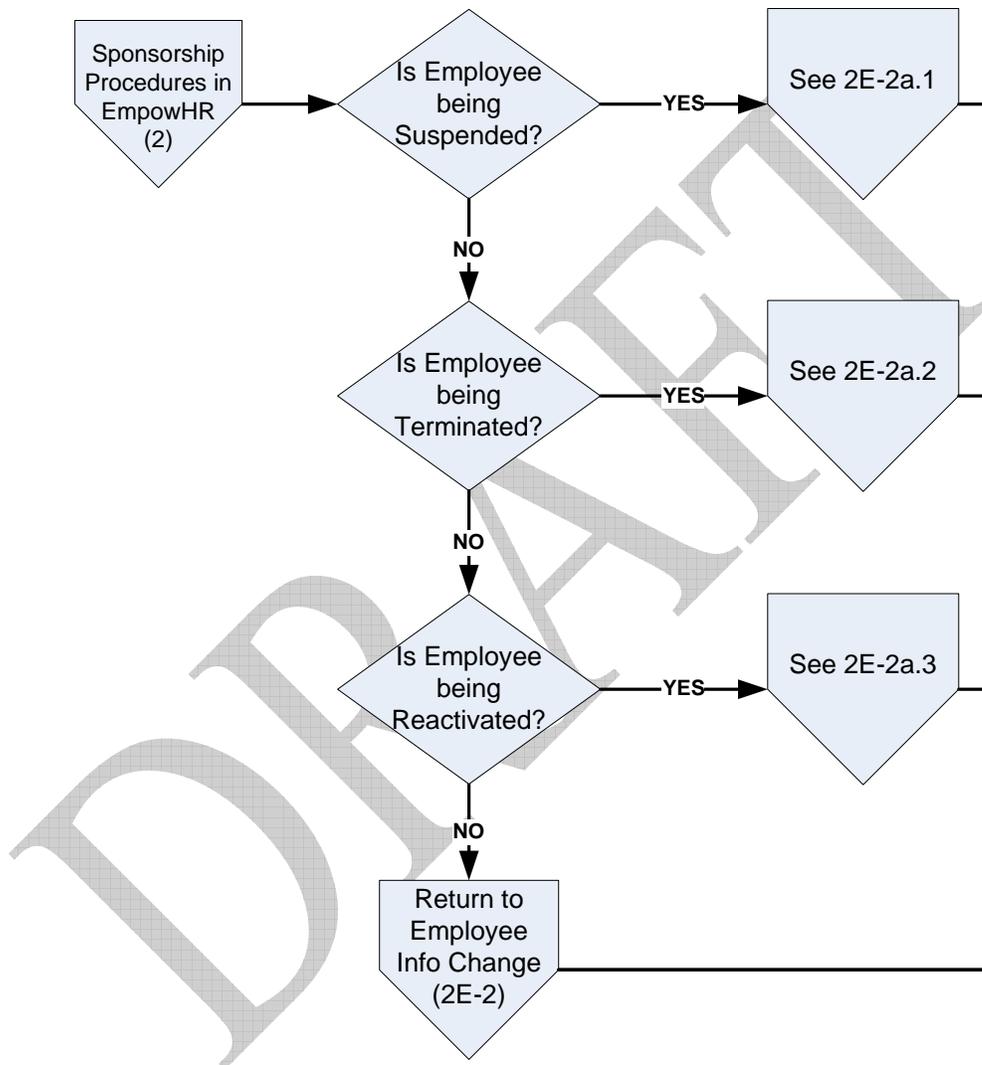


Figure 16: Employee Information Change in EmpowHR (2E-2)

1. If the Employee's employment status is to be changed, go to the Employee Status Change process (2E-2a).
2. If the Employee's "Card Required" status needs to be changed, go to the Employee "Card Required" Change process (2E-2b).
3. If there is another type of Employee information change needed, go to the Employee Other Info Change process (2E-2c).

### 5.2.4 Employment Status Change in EmpowHR

The following diagram details the workflow of the change in employment status of an existing employee in the EmpowHR system



**2E-2a**

Figure 17: Employment Status Change in EmpowHR(2E-2a)

1. If the Employee is being suspended, go to the 2E-2a.1 process.
2. If the Employee is being terminated, go to the 2E-2a.2 process.
3. If the Employee is being changed back to active from suspended or terminated, go to the 2E-2a.3 process.

### 5.2.5 Sponsorship Suspension EmpowHR

The following diagram details the workflow of card suspension by the Sponsor of an existing employee in the EmpowHR system.

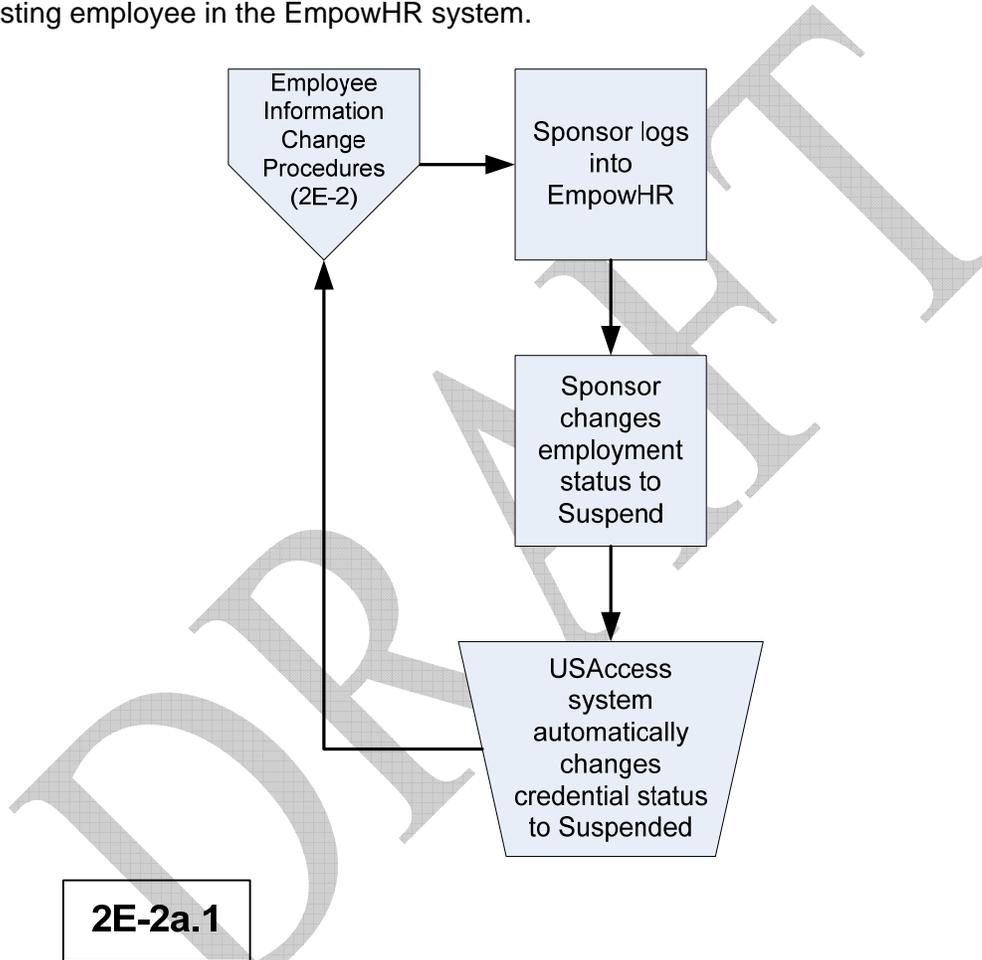
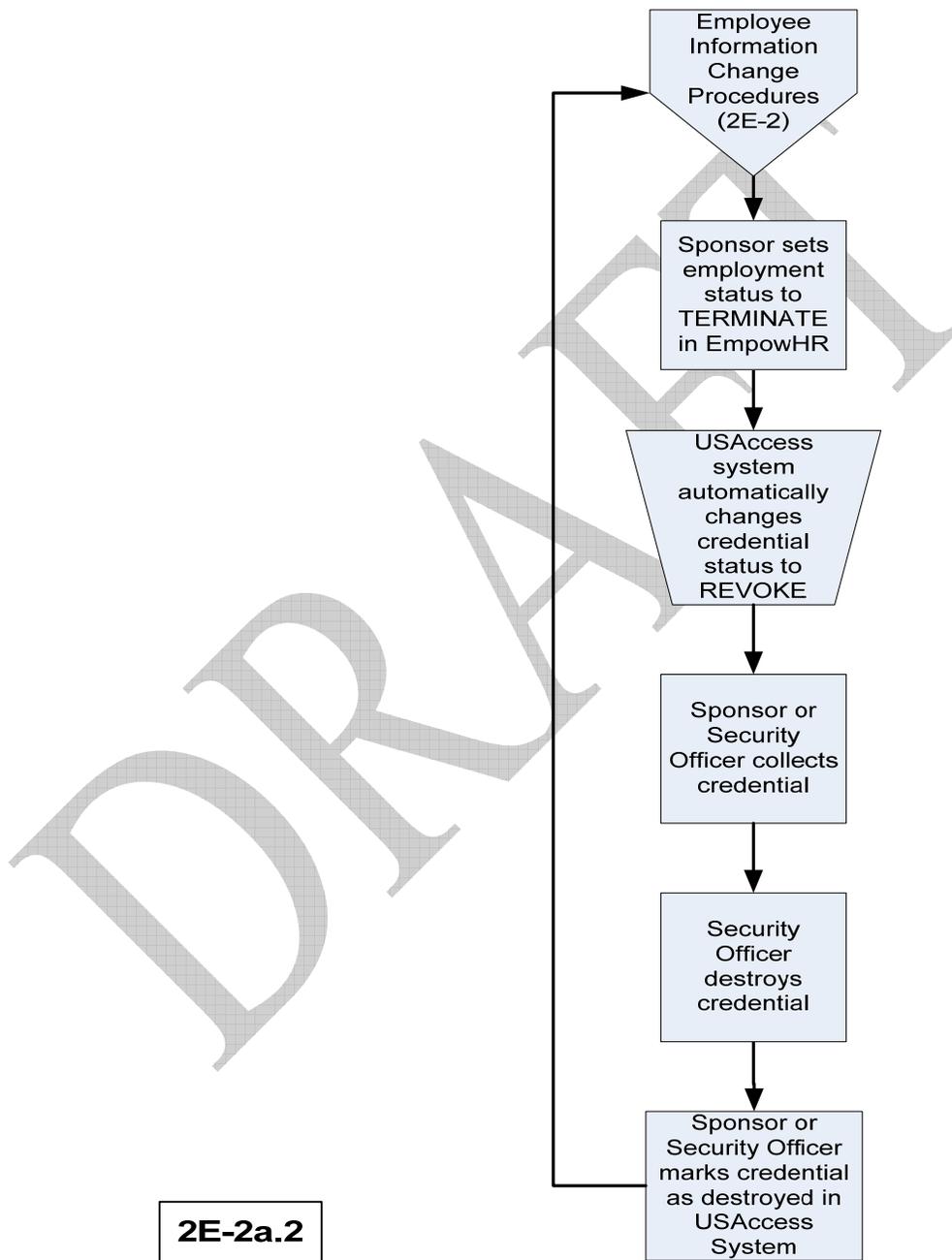


Figure 18: Sponsorship Suspension EmpowHR (2E-2a.1)

1. The Sponsor logs into EmpowHR.
2. Sponsor sets the employment status to SUSPEND and saves the record.
3. The USAccess System automatically changes the credential status to suspend.

### 5.2.6 Sponsorship Termination in EmpowHR

The following diagram details the workflow of card termination by the Sponsor of an existing employee in the EmpowHR system.



**2E-2a.2**

Figure 19: Sponsorship Termination in EmpowHR (2E-2a.2)



1. The Sponsor logs into EmpowHR.
2. Sponsor sets the employment status to TERMINATE and saves the record.
3. The USAccess System automatically changes the credential status to TERMINATE.
4. The USAccess System revokes the cardholder's certificates
5. The Sponsor or Security Officer collects the credential from the cardholder
6. The Security Officer physically destroys the credential.
7. The Sponsor or Security Officer marks the card as destroyed in the USAccess System.

DRAFT

### 5.2.7 Sponsorship Reactivation in EmpowHR

The following diagram details the workflow of card reactivation by the Sponsor of an existing employee in the EmpowHR system.

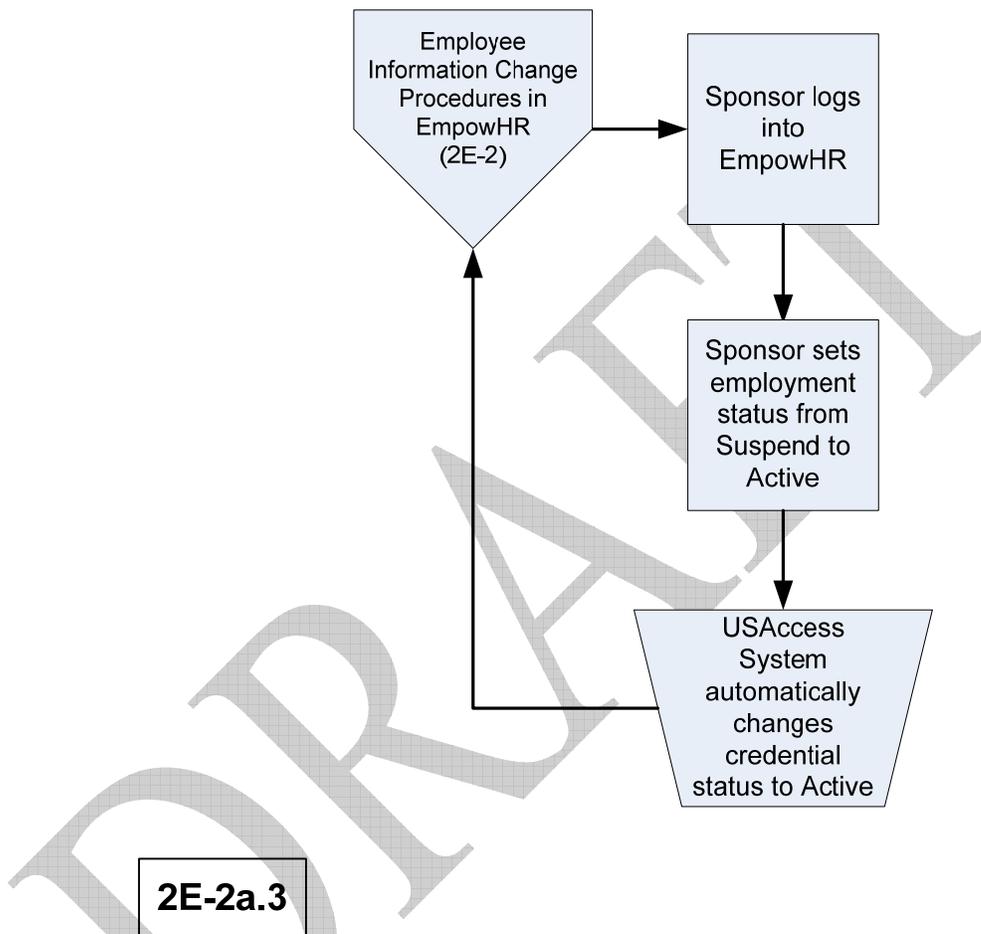
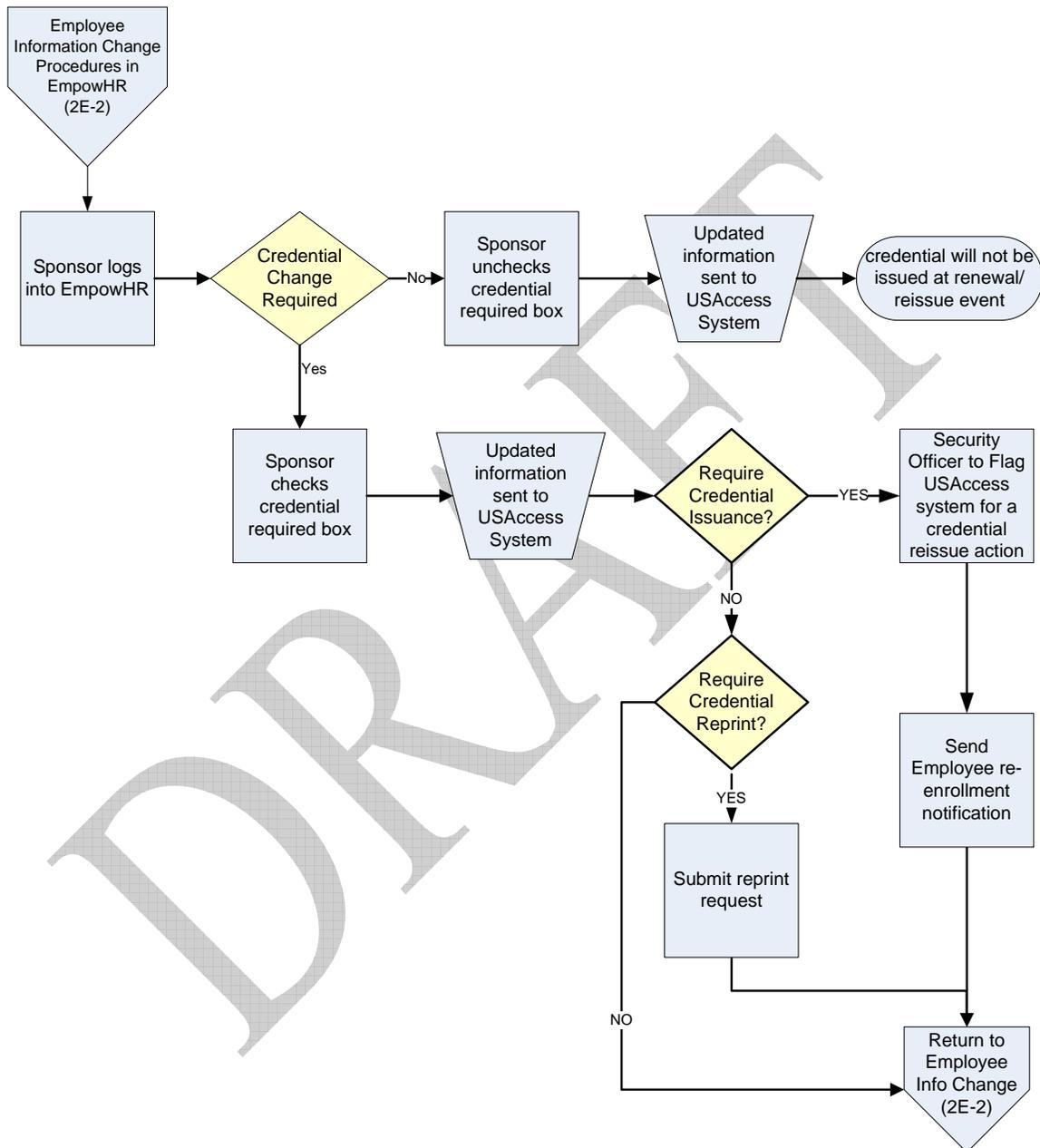


Figure 20: Sponsorship Reactivation in EmpowHR (2E-2a)

1. The Sponsor logs into EmpowHR.
2. The sponsor updates the employee status to ACTIVE through EmpowHR.
3. The USAccess System is automatically updated with the new Active status.

### 5.2.8 Employee Card Required Change in EmpowHR

The following diagram details the workflow of card change by the Sponsor of an existing employee in the EmpowHR system.



2E-2b

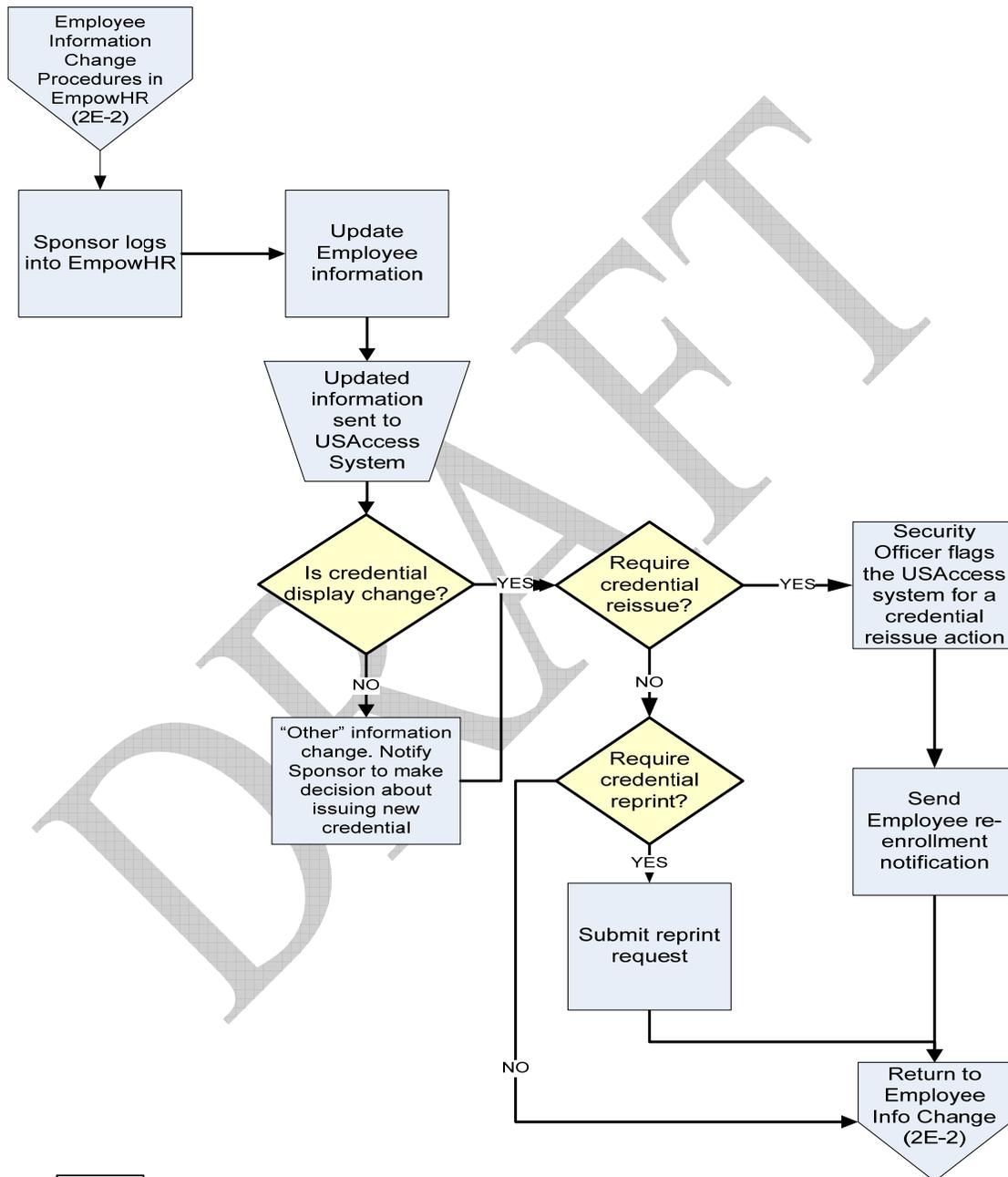
Figure 21: Sponsorship Card Required Change Process (2E-2b)

1. The Sponsor logs into EmpowHR.
2. If the “Card Required” box is checked and the Employee no longer needs a card, then the Sponsor un-checks the box.
  - a. The USAccess System is automatically updated from EmpowHR.
  - b. If the Employee is a new applicant who has not enrolled and been issued a card yet, no card will be issued or printed.
  - c. If the Employee currently holds a card, they can continue to use the card until a Reissue or Renewal event takes place; no new card will be issued then.
3. If the “Card Required” box is not checked, and the Employee needs a card, the Sponsor checks the box.
  - a. The USAccess System is automatically updated from EmpowHR.
  - b. If the Employee needs their card re-issued, the Security Officer flags the Employee for needing a card reissue in the USAccess System.
  - c. USAccess System sends notice to Employee to schedule a time to Employee Info Change Procedures (2E-2).

DRAFT

### 5.2.9 Employee Other Information Change in EmpowHR

The following diagram details the workflow of other types of information change by the Sponsor of an existing employee in the EmpowHR system.



**2E-2c**

Figure 22: Sponsorship Employee Other Information Change in EmpowHR (2E-2c)



1. Sponsor logs into EmpowHR and updates the necessary Employee information.
2. If the data that was updated is data that is displayed on the card, the Sponsor will decide if a new card needs to be issued.
  - a. The default is that no new card will be issued.
  - b. New Card Issuance
    - i. The USAccess System flags the Employee for needing a card reissue and makes them enrollment eligible.
    - ii. USAccess System sends notice to Employee to schedule a time to re-enroll
3. If the data is changed and does not affect the card display:
  - a. Sponsor is notified that the Employee's information has been changed
  - b. Sponsor decides if a new card needs to be issued; if a new card is to be issued:
    - i. USAccess System flags the Employee for needing a card reissue and makes them enrollment eligible.
4. USAccess System sends notice to Employee to schedule a time to re-enroll.

DRAFT

### 5.3 Payroll Personnel Workflows

#### 5.3.1 Sponsorship of New Employee in Payroll Personnel

The following diagram details the workflow of the first-time sponsorship of a new employee in the Payroll Personnel system

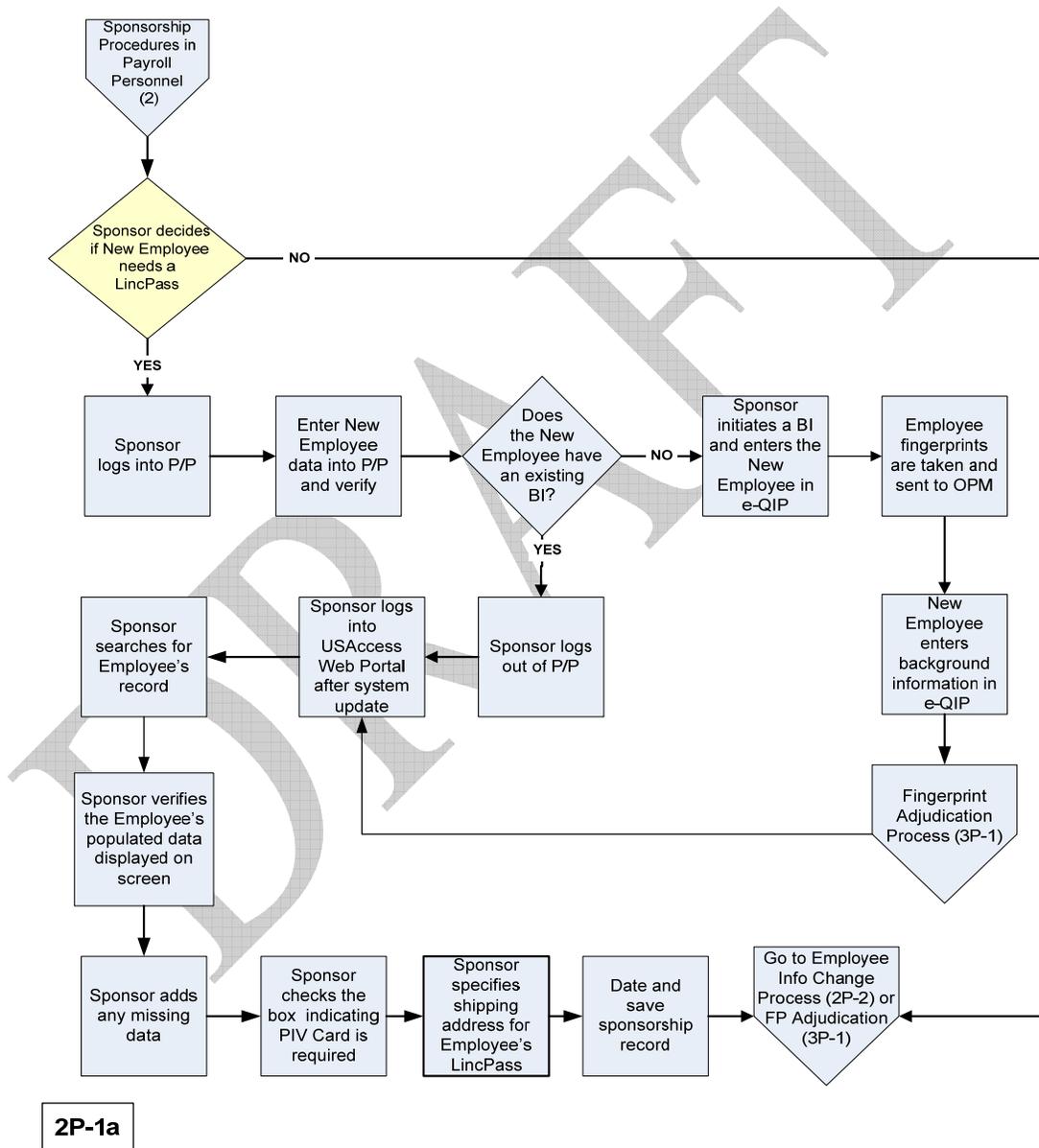


Figure 23: Sponsorship of New Employee in Payroll Personnel (2P-1a)



1. Sponsor determines if the Employee needs a LincPass using the LincPass Distribution Risk Assessment process. If one is not needed, the process stops here; otherwise the Sponsor continues.
2. Sponsor logs into Payroll Personnel.
3. Sponsor enters the Employee's information and then verifies that all information is correct.
4. If the Employee does not have an existing BI, the Sponsor initiates one by entering the Employee's information in e-QIP if accessible. If not accessible, the Sponsor uses the SP-XX paper form to initiate the BI.
  - a. The Employee's fingerprints are captured and sent to OPM for the fingerprint check.
  - b. The Employee then goes into e-QIP, if accessible to enter their information; otherwise they enter the information on the SF-XX paper form.
  - c. The Sponsorship process will move on while the Fingerprint Check is in progress (results will be evaluated during Adjudication (3P-1)).
5. If the Employee has an existing BI, the Sponsor exits Payroll Personnel and logs into the USAccess Web Portal.
6. Sponsor searches for the Employee's record and verifies that all the Employee data is correct.
7. If there is any data missing, (business email, business phone, country of citizenship, emergency response official, adjudication status and PIV card required) the Sponsor adds the data in the USAccess Web Portal.
8. Sponsor checks box indicating that a PIV card is required
9. Sponsor provides the Employee's shipping address for the LincPass.
10. Sponsor saves the record with the current date captured.
11. Sponsor goes to the Employee Information Change Process (2P-2) if the Employee's Information or Status changes; otherwise go to the Fingerprint Adjudication Process (3P-1).

### 5.3.2 Sponsorship of Existing Employee in Payroll Personnel

The following diagram details the workflow of the sponsorship of an existing employee in the Payroll Personnel system.

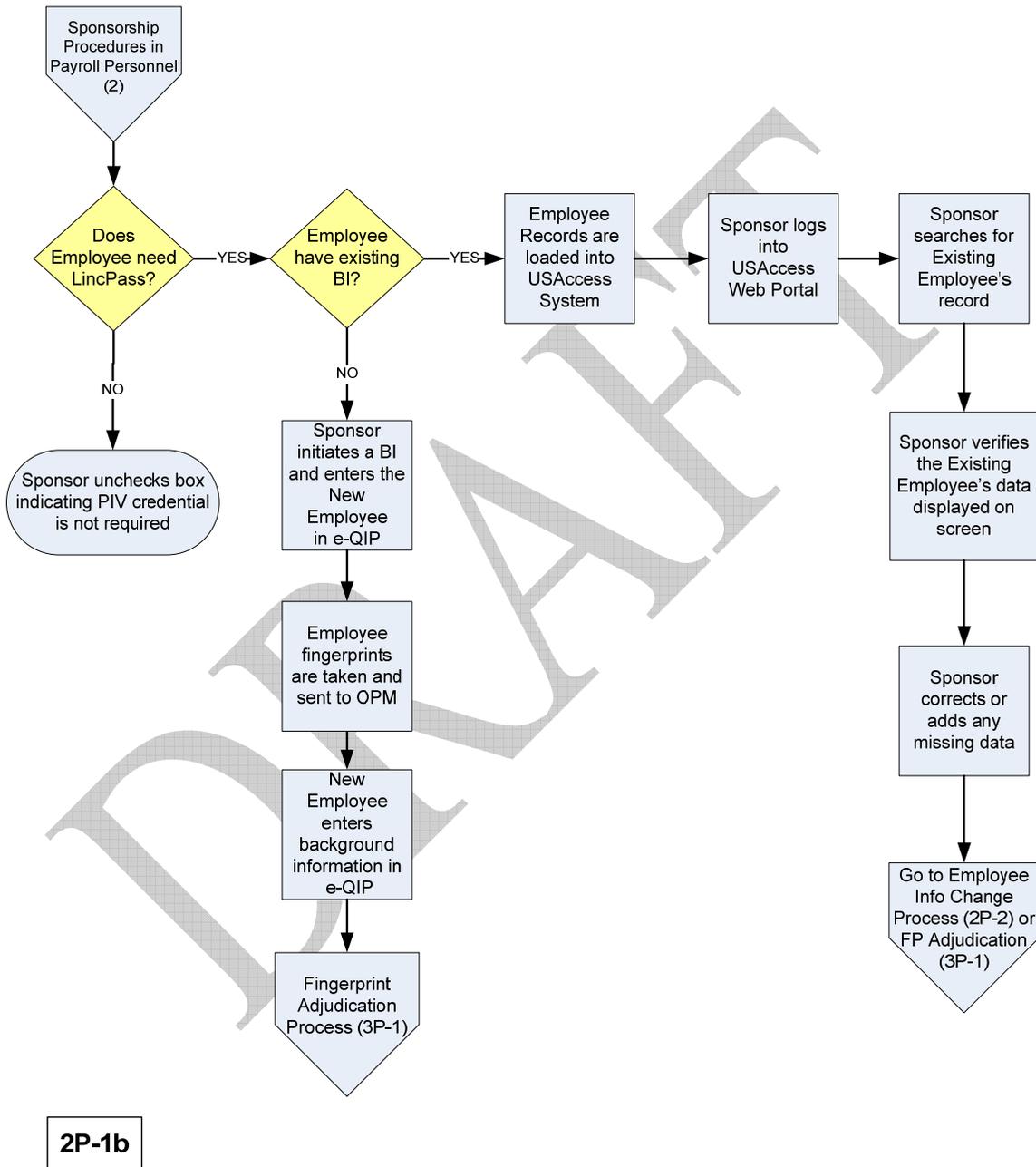
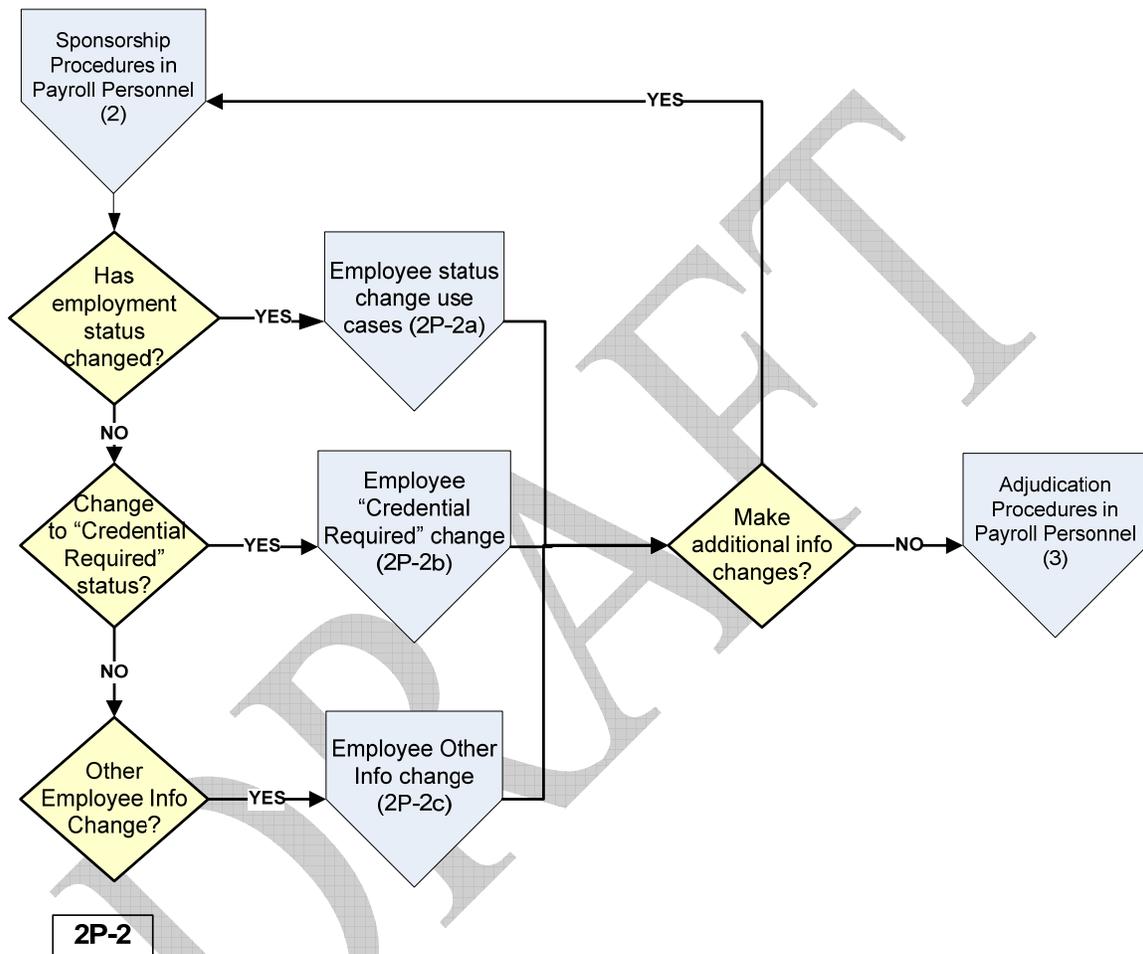


Figure 24: Sponsorship of Existing Employee in Payroll Personnel (2P-1b)

1. If the Employee does not have an existing BI, the Sponsor initiates one by entering the Employee's information in e-QIP if accessible. If not accessible, the Sponsor uses the SF-85, 85P, or 86 paper form to initiate the BI.
  - a. The Employee's fingerprints are captured and sent to OPM for the fingerprint check.
  - b. The Employee then goes into e-QIP, if accessible to enter their information; otherwise they enter the information on the SF-85, 85P, or 86 paper form.
  - c. The Sponsorship process will move on while the Fingerprint Check is in progress (results will be evaluated during Adjudication (3P-1)).
2. Employee records are uploaded to the USAccess Web Portal.
3. The Sponsor logs into the USAccess Web Portal and searches for the Employee's record.
4. The USAccess Web Portal displays the Employee's record and the Sponsor verifies that the Employee's data is correct.
5. Enter the six required fields and any other missing data, (business email, business phone, country of citizenship, emergency response official, adjudication status and PIV card required) the Sponsor adds the data in the USAccess Web Portal.
  - a. Sponsor logs back into Payroll Personnel and makes the same Employee Information updates
6. Sponsor checks box indicating that a PIV card is required, if the Employee needs a LincPass.
7. Sponsor saves the record.
8. Sponsor goes to the Employee Information Change Process (2P-2) if the Employee's Information or Status changes; otherwise go to the Fingerprint Adjudication Process (3P-1).

### 5.3.3 Employee Information Change in Payroll Personnel

The following diagram details the workflow of information change of an existing employee in the Payroll Personnel system.



**2P-2**

Figure 25: Sponsorship Employee Information Change in Payroll Personnel (2P-2)

1. If the Employee’s employment status is to be changed, go to the Employee Status Change process (2P-2a).
2. If the Employee’s “Card Required” status needs to be changed, go to the Employee “Card Required” Change process (2P-2b).
3. If there is another type of Employee information change needed, go to the Employee Other Info Change process (2P-2c).

### 5.3.4 Employee Status Change in Payroll Personnel

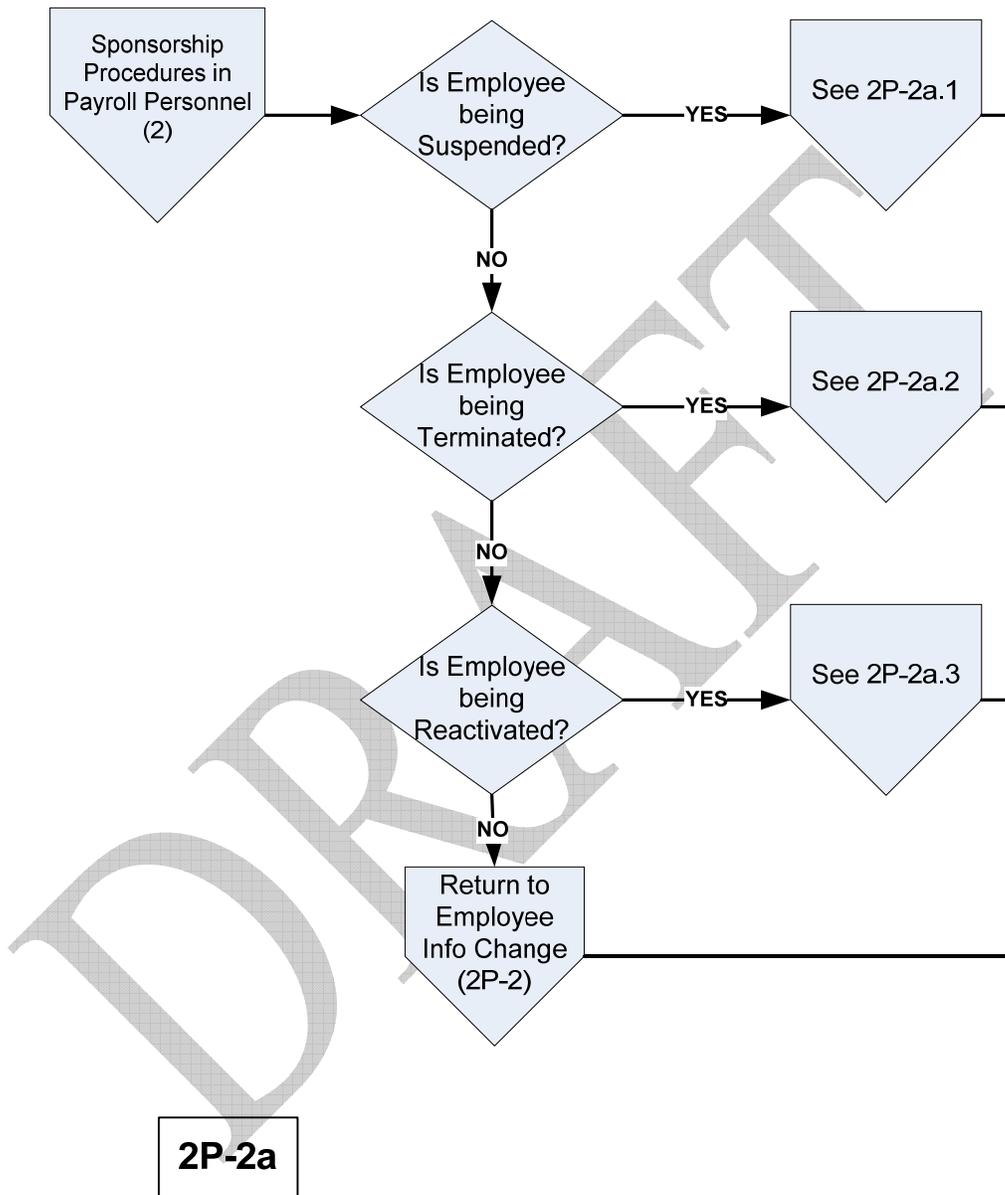


Figure 26: Sponsorship Employee Status Change in Payroll Personnel (2P-2a)

1. If the Employee is being suspended, go to the 2P-2a.1 process.
2. If the Employee is being terminated, go to the 2P-2a.2 process.
3. If the Employee is being changed back to active from suspended or terminated, go to the 2P-2a.3 process.

### 5.3.5 Sponsorship Suspension in Payroll Personnel

The following diagram details the workflow of card suspension by the Sponsor of an existing employee in the Payroll Personnel system.

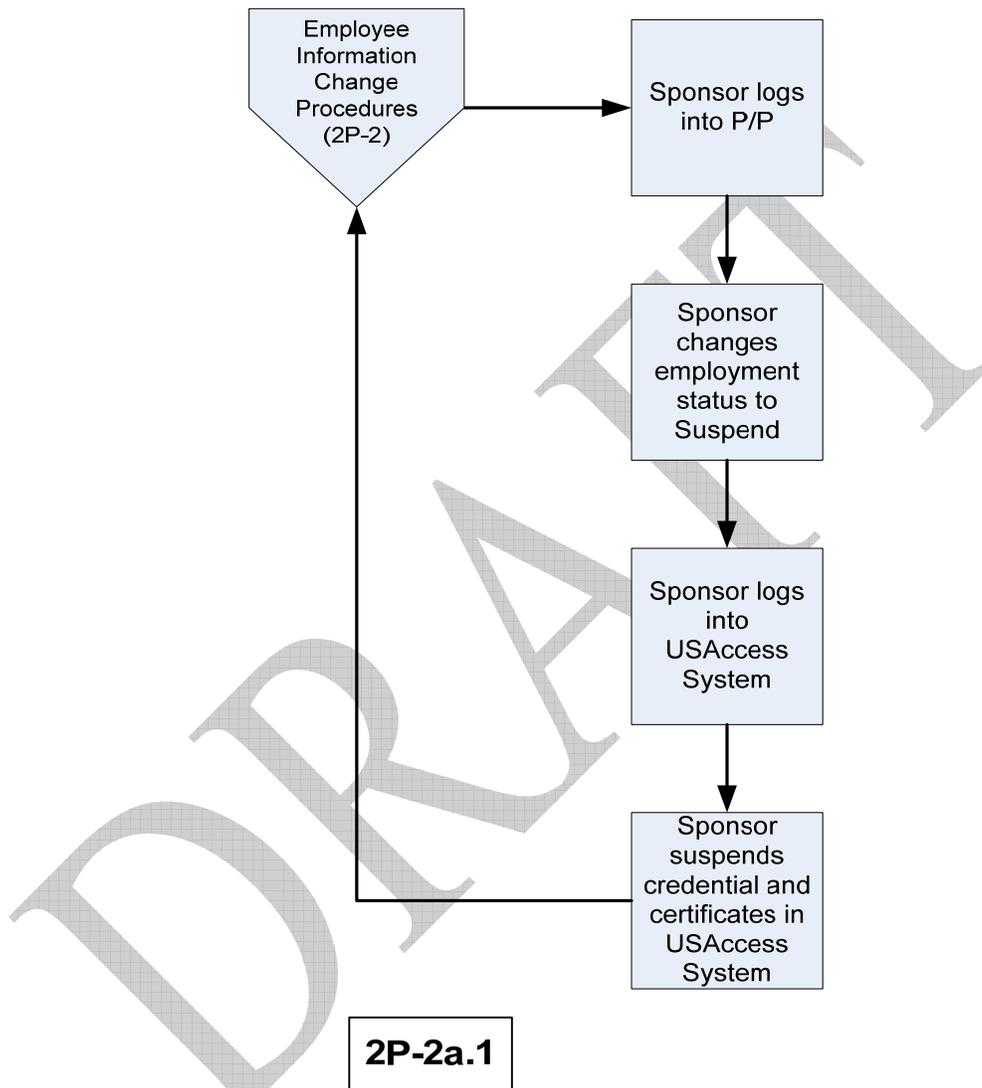


Figure 27: Sponsorship Suspension in Payroll Personnel (2P-2a.1)

1. The Sponsor logs into Payroll Personnel
2. Sponsor sets the employment status to SUSPEND and saves the record.
3. Sponsor logs into USAccess System
4. Sponsor changes the credential status to suspend in the USAccess System.

### 5.3.6 Sponsorship Termination in Payroll Personnel

The following diagram details the workflow of card termination by the Sponsor of an existing employee in the Payroll Personnel system.

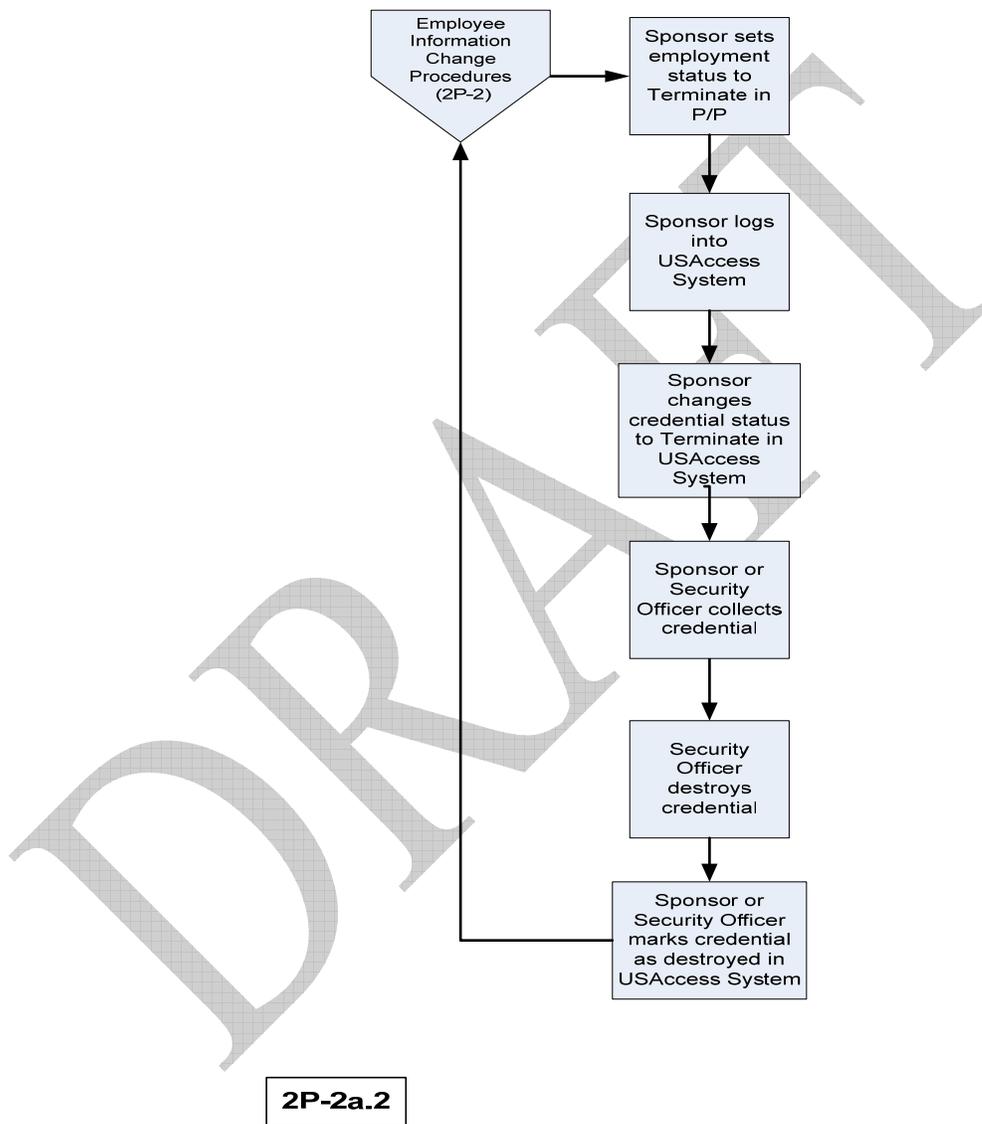


Figure 28: Sponsorship Termination in Payroll Personnel (2P-2a.2)

1. The Sponsor logs into Payroll Personnel
2. Sponsor sets the employment status to TERMINATE and saves the record.
3. Sponsor logs into the USAccess System.



4. Sponsor changes the credential status to TERMINATE in USAccess System.
5. The USAccess System revokes the cardholder's certificates
6. The Security Officer or Sponsor collects the credential from the cardholder.
7. The Security Officer physically destroys the credential.
8. The Security Officer or Sponsor marks the card as destroyed in the USAccess System.

DRAFT

### 5.3.7 Sponsorship Reactivation in Payroll Personnel

The following diagram details the workflow of card reactivation by the Sponsor of an existing employee in the Payroll Personnel system.

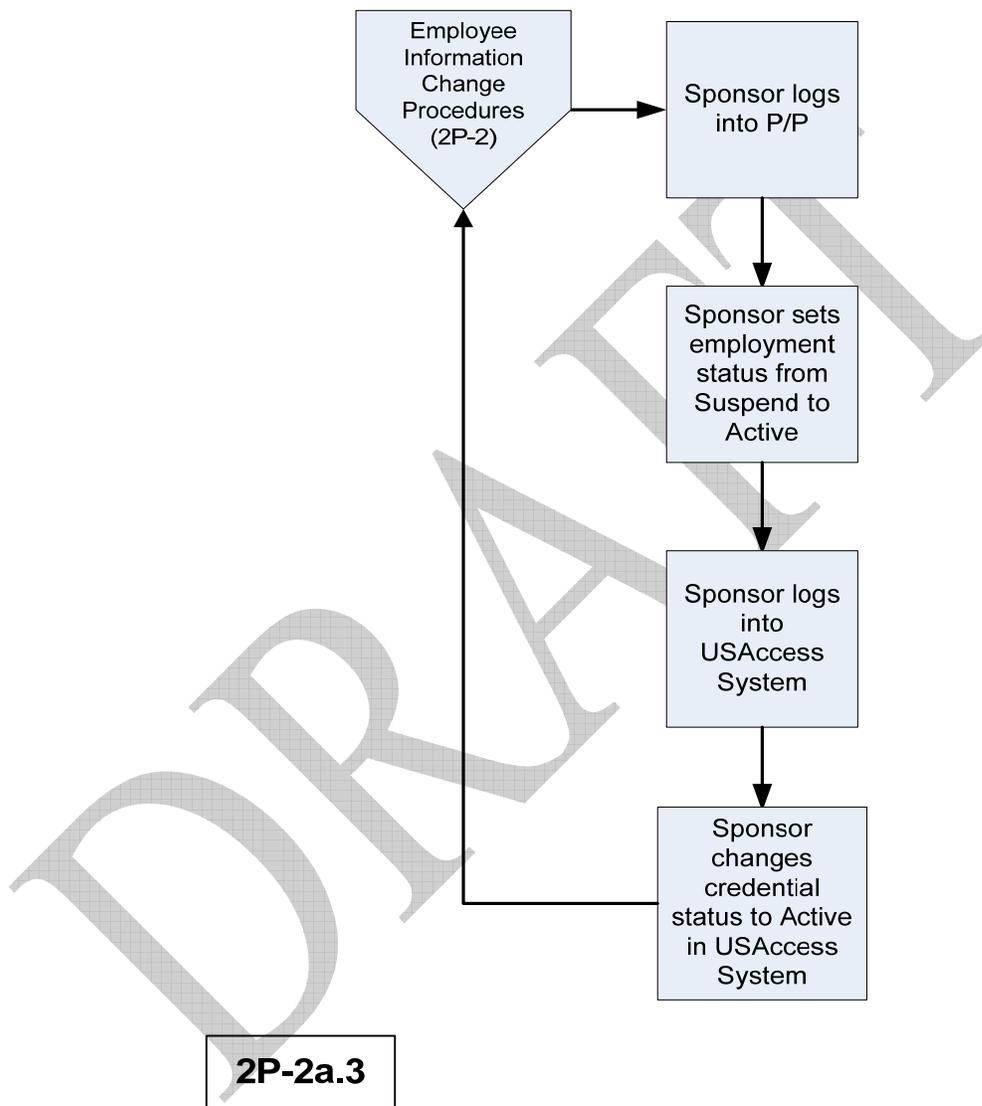
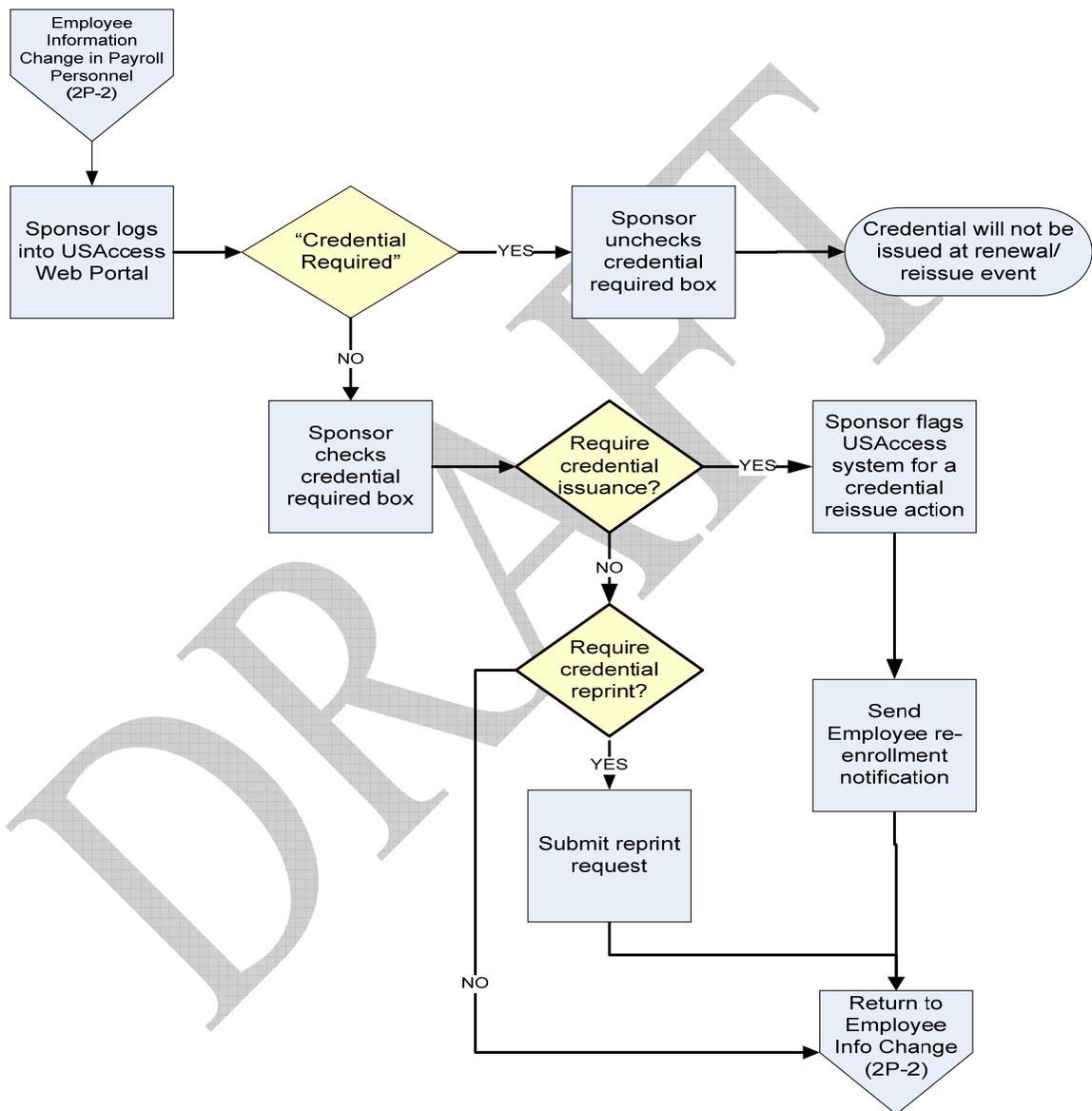


Figure 29: Sponsorship Reactivation in Payroll Personnel (2P-2a.3)

1. Sponsor logs into Payroll Personnel
2. The sponsor updates the employee status to ACTIVE.
3. Sponsor logs into USAccess System.
4. Sponsor reactivates the card and certificates in USAccess System.

### 5.3.8 Employee “Card Required” Change in Payroll Personnel

The following diagram details the workflow of card change by the Sponsor of an existing employee in the Payroll Personnel system.



**2P-2b**

Figure 30: Sponsorship Employee “Card Required” Change in Payroll Personnel (2P-2b)

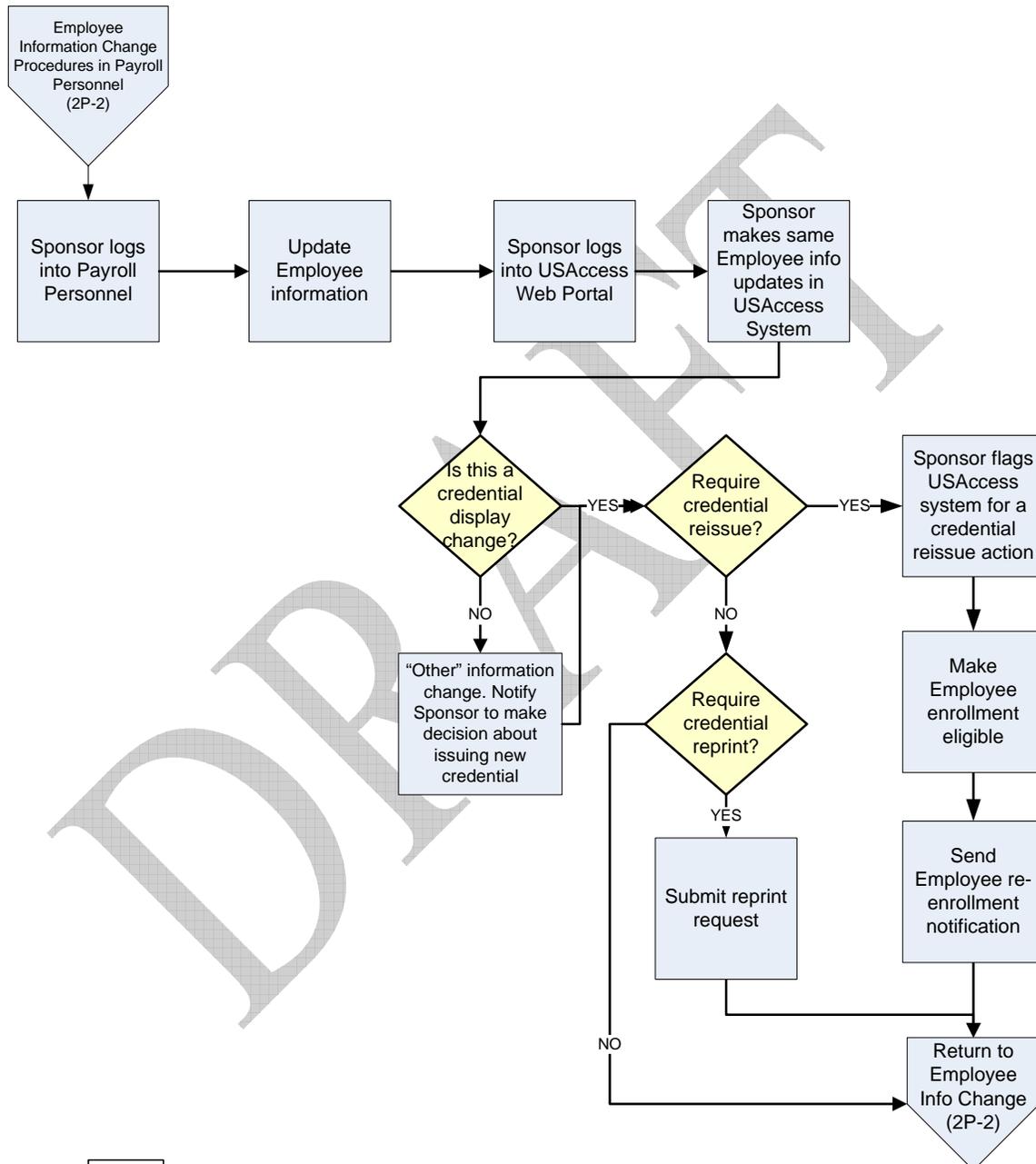
1. The Sponsor logs into the USAccess Web Portal.

2. If the “Card Required” box is not checked, and the Employee needs a card, the Sponsor checks the box.
  - a. If the Employee needs their card re-issued, the Sponsor flags the Employee for needing a card reissue in the USAccess System.
  - b. The USAccess System makes them enrollment eligible.
  - c. USAccess System sends notice to Employee to schedule a time to re-enroll.
3. If the “Card Required” box is checked, and the Employee no longer needs a card, the Sponsor un-checks the box.
  - d. If the Employee is a new applicant who has not enrolled and been issued a card yet, no card will be issued or printed.
  - e. If the Employee currently holds a card, they can continue to use the card until a Reissue or Renewal event takes place; no new card will be issued then.

DRAFT

### 5.3.9 Employee Other Information Change in Payroll Personnel

The following diagram details the workflow of other types of information change by the Sponsor of an existing employee in the Payroll Personnel system.



2P-2c

Figure 31: Employee Other Information Change in Payroll Personnel (2P-2c)

1. Sponsor logs into Payroll Personnel and updates the necessary Employee information.
2. Sponsor makes the same updates to the Employee's information in the USAccess System.
3. If the data that was updated is data that is displayed on the card, the Sponsor will decide if a new card needs to be issued.
  - a. The default is that no new card will be issued.
  - b. New Card Issuance
    - i. The USAccess System flags the Employee for needing a card reissue and makes them enrollment eligible.
    - ii. USAccess System sends notice to Employee to schedule a time to re-enroll.
4. If the data does not change, does not affect the card display:
  - c. Sponsor is notified that the Employee's information has been changed
  - d. Sponsor decides if a new card needs to be issued; if a new card is to be issued:
    - iii. USAccess System flags the Employee for needing a card reissue and makes them enrollment eligible.
5. USAccess System sends notice to Employee to schedule a time to re-enroll.

#### **5.4 Request Card Re-Issuance**

When personal data is updated in the USAccess web portal, not related to card display, employment status, and card required data elements, no additional actions are required by the USAccess System. Updates to these data elements are saved to the Identity record and shall reflect across all agencies. A change to an applicant's personal information triggers a notification to the all sponsors for this applicant so a decision can be made by each individual sponsor if a new card needs to be issued.

### 5.4.1 Sponsorship Re-Issuance Process

The following diagram details the workflow card re-issuance by the Sponsor of an existing employee.

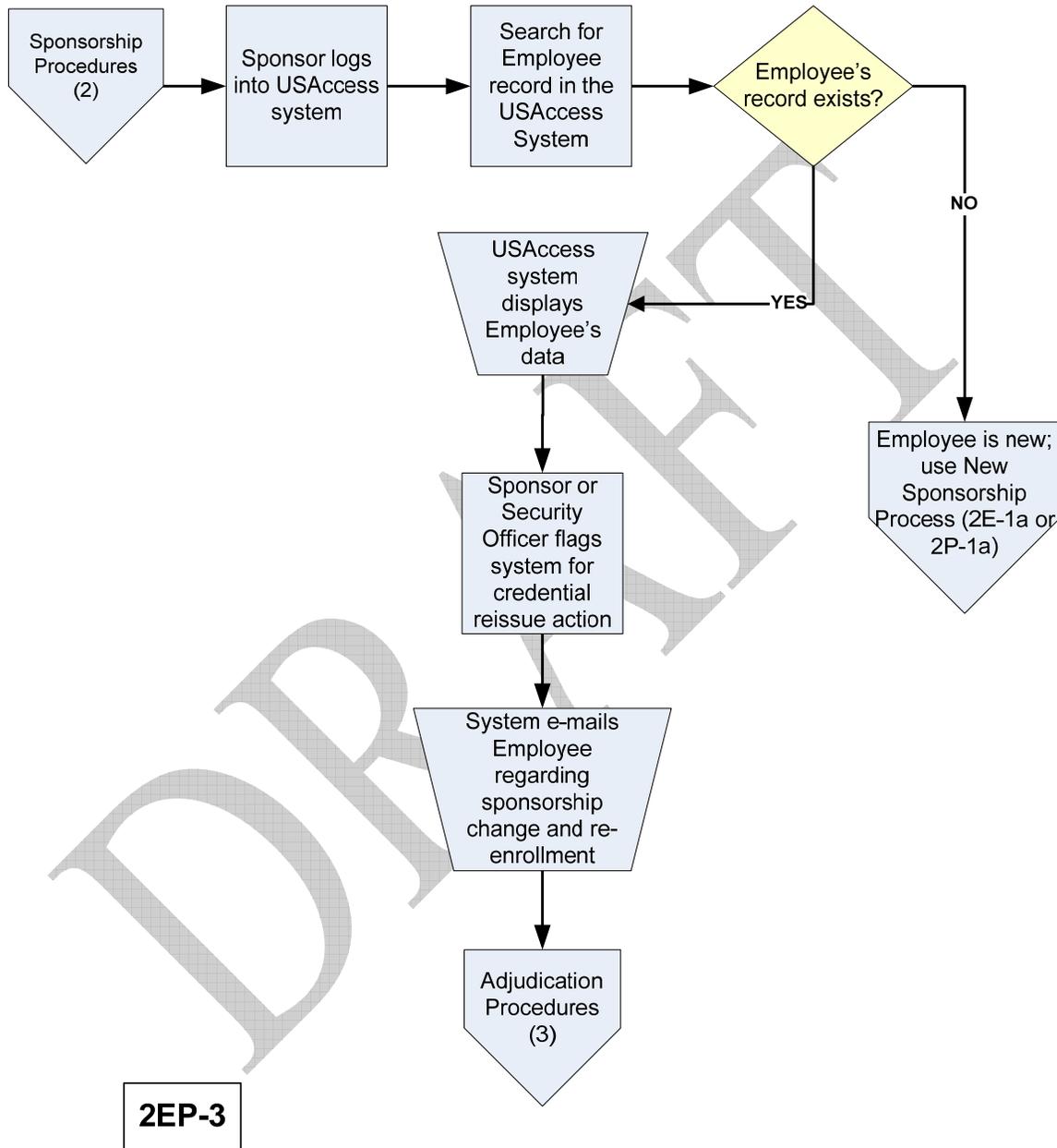


Figure 32: Sponsorship Re-Issuance (2EP-3)

In the case of re-issuance, the entire enrollment and issuance process, including fingerprint and facial image capture, shall be conducted. [Note: Because of the geographic locations of the agencies in USDA, management is going to NIST to request

changing this. It is hoped that an employee would not have to drive back to an enrollment station for a re-issuance. The Sponsor and security officer shall have the ability to initiate a credential re-issue.

1. The sponsor logs onto the USAccess web portal.
2. Sponsor searches for the applicant to determine if they are a new or existing applicant. If they are new, use the New Employee Sponsorship process to set them up in the USAccess System (2E-1a or 2P-1a depending on the Agency's authoritative HR system).
3. USAccess System displays the applicant record in sponsorship screen.
4. Sponsor or Security Officer flags USAccess System for a credential reissue action.
5. USAccess System automatically notifies the applicant of the sponsorship change and re-enrollment via e-mail. The e-mail will contain the sponsorship information so that the applicant can verify the accuracy of the data and shall provide enrollment instruction

DRAFT

## Section 6 Sponsorship Policies

### 6.1 Sponsor Responsibilities

Sponsors are individuals who act on behalf of the Department to request LincPass credentials for USDA Applicants (employees, contractors, or affiliates). Depending on the Applicant's employment status, a Sponsor may be a federal supervisor, contracting officer, contracting officer's representative, or other federal official. The Sponsor must have training and a LincPass in order to perform HSPD-12 Sponsor functions.

The Sponsor's basic responsibilities are to:

- Conduct identity proofing.
- Determine applicant's need for a LincPass.
- Review the Applicant's SF-85, SF-86 or SF 85P, Questionnaire for Non-Sensitive Positions, and OF-306, Declaration for Federal Employment (unless the SF-85 is done in e-QIP).
- Enter applicant's information into EmpowHR or P/P.
- Modify records for applicants based on updates to user status and relevant information.
- Suspend or revoke LincPass via the USAccess web application.
- Initiate re-enrollments for current or previous cardholders.
- When required, recover the credential from the Applicant.

### 6.2 Sponsor Training

#### 6.2.1 Resources for Initiating NACIs

HR Directors will receive the following documents in electronic format to assist with initiating NACIs:

- OPM Publication IS-15, Requesting OPM Personnel Investigations.
- OPM's SF-85 and OF-306 Accept Guidelines.
- USDA PDSD Checklist and Transmittal memo to inform PIV Sponsors what corrections are needed to forms.

#### 6.2.2 Training for I.D. Validation

- Sponsors will be given FAQs similar to the information in the Identity Proofing section 5.3 in this document. For further training they can read pages 2-3 of the Driver's License Guide and review states' drivers license formats.
- Sponsors should complete the HSPD-12 implementation training module, read the Q&A, and stay alert to identity and I.D. fraud as an on-going crime. Read pages 2-3 of the Driver's License Guide

- Review the formats of State's SDL. Finally, become familiar with State's SDL validation points as shown in the Driver's License Guide.

#### **6.2.4 USACCESS Web Application Training**

Sponsors will receive training on using the USAccess web application to enter applicant's information. If in EmpowHR, Sponsors will receive training on the new HSPD-12 features in EmpowHR.

### **6.3 Identity Proofing**

Applicants are required to show the sponsor two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents shown on Form 1-9 (see [Appendix B](#)), Employment Eligibility Verification. At least one document shall be a valid State or Federal government-issued picture ID card. Applicants who possess a current State Drivers License or State Picture ID card shall present that document as one identity source document before presenting other State or Federal government-issued picture ID cards. For example, an Applicant might show his or her State Drivers License and a military reserve ID card as proof of identity.

If an ID does not seem genuine or relate to the person presenting it, the Sponsor asks a supervisor to review the IDs. If concerns still remain, the ID is photocopied returned to the Applicant, and the Applicant is told that an additional review will be required.

Applicants are required to provide two forms of identification in original form. The identification documents must come from the list of acceptable documents shown on Form 1-9, Employment Eligibility Verification. At least one I.D. shall be a valid State or Federal government-issued picture ID. Applicants who possess a current State Driver's License or State Picture ID (hereafter, SDL) should be asked to present that ID before accepting other federal or state-issued picture IDs.

The responsibilities are different for a Sponsor depending on whether or not the Applicant has a background investigation. Sponsors will check to verify if employees and contractors already have favorably adjudicated background investigations via OPM for employees or through prior agency HR or Security offices for contractors. For those individuals, only identity proofing is conducted. For employees and contractors who do not have a background investigation, background investigations will be initiated using the same procedures as for a new USDA employee or contractor.

Whenever individuals holding LincPasses end their employment or work with the Department, the Applicant must return their LincPasses and other properties belonging to USDA. On occasion, the agency Adjudicator will notify him/her that all or part of an Applicant's background investigation was unsuccessfully adjudicated, and that a proposed notice of denial or revocation of the LincPass will be issued.

### 6.3.1 Disqualifying Information

The Sponsor will contact the Applicant to discuss potentially disqualifying information. Examples of potentially disqualifying information include, but are not limited to:

- Use, possession, supply, or manufacture of illegal drugs in the last year. (See Q14 on the SF-85 for examples of illegal drugs).
- Conviction, imprisonment, probation, or parole during the last 10 years (includes felonies, firearms or explosive violations, misdemeanors, and all other offenses). (See Q9 on the OF-306).
- Conviction by military court-martial in the past 10 years. (See Q10 on the OF-306).
- Currently under charges for any violation of law. (See Q11 on the OF-306).
- Fired from any job during the last 5 years. (See Q12 of the OF-306 for conditions involving separation from employment that must be reported.)
- Current delinquency on any Federal debt. (See Q13 on the OF-306 for a specific explanation of the kind of delinquencies that must be reported.)

### 6.3.2 ID Card Examination and Validation

The purpose of I.D. examination and validation is to determine whether an ID appears genuine (free of signs of alteration or counterfeiting) and relates to the person presenting it. If an ID reasonably appears on its face to be genuine and to relate to the person presenting it, no further review is needed. The ID is acceptable. When there is doubt about the authenticity of an identification card, a valid version of that identification card must be available for comparison. Valid versions of the 50 States driver's licenses and other commonly used IDs are shown in the U.S. and Canada I.D. Checking Guide (Driver's License Guide).

### 6.3.3 IDs Applicants Are Required to Present for LincPasses

Applicants are required to provide two forms of identification in original form. The identification documents must come from the list of acceptable documents shown on Form 1-9, Employment Eligibility Verification. At least one I.D. shall be a valid State or Federal government-issued picture I.D. Along with social security numbers, State Issued Driver's Licenses (SDL's) are the most common form of I.D. used in the U.S. With few exceptions, Applicants will have a SDL that can be properly validated. In addition, almost all states have tamper resistant SDL's. Using tamper resistant SDL's makes the I.D. validation process more reliable.

### 6.3.4 I.D. Validation Challenges

If the Applicant does not have an SDL, the Applicant needs to show two other forms of ID (hereafter, Other IDs or OID) in original forms that are listed in the I-9. At least one document must be a valid State or Federal government-issued picture ID. Picture IDs or other IDs will not be accepted unless they are listed on the I-9.

Some of the challenges in validating SDL/OIDs are:

- Individual states have 1 to 3 valid SDL formats in use at one time. The Sponsor may not have seen one or two of the valid formats.
- Some states' renewal rules allow use of the same facial photograph for up to 10 years.
- SDL/OIDs become worn over time which makes them more difficult to validate.
- Unfamiliar SDL's may require more time to validate.

### 6.3.5 Altered SDL/OIDs

Altered IDs may exhibit signs of tampering in one or more places, including the numbers, the photograph, and the laminate. The birth date, driver's license number, height, and weight may be scratched or bleached out and inked over or cut out and reinserted. If altered, the numbers may be bumpy.

Altered I.D. cards and documents may also have erasures, strikeouts, or pen-and-ink changes. A photograph with bumpy surfaces or rough edges may have been inserted over the original. The SDL surface should be flat. A test of this surface can be made by tracing one finger lightly over the front surface of the SDL and noting if the surface is raised at any point, particularly where the facial photograph is located.

Because many states place their seal over the photograph, an I.D. altered in this manner would cover part of the seal.

Changes in the card's laminated cover often indicate tampering. It may contain glue lines or rough edges, especially near the photograph. Altered numbers may not match up after the laminate is put back into place. A shadowy or cloudy image on the card means that a new laminate covers the original.

### 6.3.6 Counterfeit SDL/OIDs

For the most part, fake or counterfeit IDs encompass two different types. Some closely resemble state driver's licenses. Others, such as identification cards manufactured by mail-order firms, may have no legal counterpart, making illegal ones harder to detect. Still, both types of counterfeit cards may contain anomalies that can alert officials to their lack of authenticity. For example, a fake driver's license, when compared to the real thing, may be a different size, thickness, or color. Letters and numbers may differ in size, typeface, or placement. In fact, although many counterfeiters spend a great deal of time reproducing the front of the card, they may merely photocopy the reverse side, leaving blurred letters and/or dark images.

No matter how professional-looking it is, the front of the counterfeit card may miss the mark. The photograph may lack the quality of the motor vehicle card, producing a shadow or glare or giving the subject "red-eye." Finally, the state seal or logo may be missing or altered. Mail-order IDs may actually contain such phrases as "for personal

use,” “office use only,” or “not a government document,” a sure sign that the card is a fake.

A poorly counterfeited SDL/OID may also have printing that is not clear, distinct, or sharp. There may be uneven spacing or misalignment of type. Colors may not be clear or well-defined. The hologram on the SDL may not show different images when the angle of the viewing is changed. In contrast, genuine SDL/OIDs have printing that is crisp and well-defined and holograms that show different images when the angle of the viewing is changed.

Examples of counterfeit features can be found at [www.secretservice.gov/money\\_detect.shtml](http://www.secretservice.gov/money_detect.shtml). Although the examples shown are counterfeit money, the same signs of counterfeiting can apply to SDL/OIDs.

### **6.3.7 Borrowed SDL/OIDs**

While physical appearance changes may be due to aging, injury, cosmetic surgery, or other reasons, the changes may also be due to use of a borrowed ID. Even subtle differences between the person presenting the I.D. and the photograph and/or the physical description data on the card should be questioned. Persons performing identity proofing will look for duplicate and expired cards. An expired driver’s license cannot be accepted. Be wary of SDL’s marked “DUPL” because they may not belong to the person presenting it as identification.

### **6.3.8 I.D. Validation Resources**

The Driver’s License Guide has authentic versions of SDL formats shown in true size and color for all 50 U.S. States and Territories and the 10 Canadian Provinces. In addition, the Guide contains authentic versions of State Identification Cards, U.S. immigration I.D. cards, U.S. military I.D. cards, and each of the U.S. States’ policy on extension of expiration dates for SDL’s held by military personnel are shown. At this writing the cost is \$13.15 plus shipping. It is valid for one year and must be repurchased on or about February 1 of each year. A website shows updates between printings. See: [www.idcheckingguide.com](http://www.idcheckingguide.com)

To validate passports, certificates, or U.S. immigration picture I.D. cards shown under “List A” of the I-9, Sponsors/Adjudicators will use the Driver’s License Guide if the I.D. documents are shown in the Guide. The Sponsor will schedule a records check on all List A documents. Picture I.D. cards and other identification documents shown under “List B” of the I-9 are validated using the Driver’s License Guide if the I.D. cards are shown in the guide. For documents not shown in the Driver’s License Guide, or issued by the U.S. federal or a state government, e.g., school, day-care, and hospital-issued records. The Sponsor will schedule a records check on all List B documents when possible.

## 6.4 Background Investigations

A National Agency Check with Inquires (NACI) is the minimum background investigation that must be performed for all applicable Federal employees, contractors, and affiliates, who require unaccompanied access to federally controlled facilities and information systems. Some positions require 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).

A NACI is (1) a search of the fingerprint and investigative files of the Federal Bureau of Investigation and other records held by federal agencies such as the U.S. Office of Personnel Management (OPM), and (2) written inquires of current and past employers, schools attended, references, and local law enforcement authorities. A LincPass may be issued after a FBI fingerprint check is completed and successfully adjudicated. However, the NACI must still be completed and successfully adjudicated for individuals to maintain eligibility to hold the credential.

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.

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 for NS BIs are scheduled as required through PSDS.

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.

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.

Applicants shall submit SF-85 forms via OPM's Electronic Questionnaire for Investigations Processing (e-QIP) system located on the OPM secure website when available. Use of e-QIP must be facilitated by agency human resources or other designated representatives. Completing e-QIP 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.

Agencies must verify that "applicable employees and contractors" have a record of a favorably adjudicated NACI. If no record of a previous NACI exists for an individual, agencies must conduct the appropriate level of investigation as required by the position

designation. “Applicable employees and contractors” are individuals who require unaccompanied access to federally controlled facilities or information systems.

On March 1, 2006, USDA Human Resources Directors were provided OPM’s records of USDA employees with 15 or less years of federal service having a NACI record as of December 6, 2005. These records are official. If individuals have had a break in service of more than two years following their last investigation, they will need the appropriate level of investigation for the position currently applied for or held. This requirement also applies to contractors having a break in service of more than two years from employment under a Federal contract.

Except in a relatively small number of cases, NACI records in electronic format for employees with over 15 years of federal service are not available. OPM deletes most NACI records 15 years after the NACI was completed. (NACIs containing serious issues are deleted after 25 years). To verify completion of a NACI that is more than 15 years old, if the employee’s name and a record of a completed NACI were not in the OPM records provided on March 1, 2006, a review of that individual’s Official Personnel Folder (OPF) or other actions may be needed to obtain such a record. OPF reviewers should look for the following when searching for evidence that a NACI was completed:

- Certificate of Investigation Notices. Beginning or about April 1, 1990, OPM began issuing a “Certificate of Investigation Notice” when an OPM NACI was completed. The Certificate was filed with the permanent OPF records. If such a certificate is found in an employee’s OPF the agency has verified the previous NACI and no additional investigation is required for Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification for Federal Employees and Contractors, implementation purposes.\* If an OPM “Closed-Discontinued Notice” or “Closed-Incomplete Notice” is the only record of a previous NACI found in the OPF, a new investigation must be scheduled.
- Documents stamped Processed Under E.O. 10450. Prior to April 1, 1990, OPM and the former U.S. Civil Service Commission, rubber stamped on certain documents were words to the effect of “Processed Under E.O. 10450,” “Stamped E.O. 10450,” or similar references to E.O. 10450 requirements being met. The stamped impression can be found on the upper right hand edge of either the former SF-171, Application for Federal Employment, OF-612, Optional Application for Federal Employment, or SF-85, Questionnaire for Nonsensitive Positions filed with the permanent OPF records. If such a stamped document is found in an employee’s OPF the agency has verified the previous NACI and no additional investigation is required for HSPD-12 implementation purposes.
- Other Federal Background Investigation Record Notices. Federal agencies with delegated authority from OPM to conduct their own background investigations developed their own forms, memos, or other materials to document the date a background investigation was completed. If such documents are located in an employee’s OPF, the agency has verified the previous background investigation and no additional investigation is required for HSPD-12 implementation purposes.

- Security/Suitability Clearance Documents. Certificates documenting the previous background investigation and granting of a security clearance, or eligibility to hold a public trust position, verifies the previous background investigation, and no additional investigation is required for HSPD-12 implementation purposes.
- SF-75 Data. If none of the above reveals a record of a previous NACI, the temporary OPF records may contain an SF-75, Request for Preliminary Employment Data. Section K, Security Data, of that form should be reviewed. If the SF-75 verifies the previous NACI no additional investigation is required for FISP-12 implementation purposes.

## 6.5 Scheduling NACIs

An advanced FBI fingerprint check can be obtained by inserting a “R” in the “Codes” block at the top of page 1 (above the “Agency Use Only” section) of the SF-85 or in the first field of the Agency Use portion of the Electronic Questionnaires for Investigations Processing (e-QIP) form . The FBI fingerprint check results are usually completed and returned to your agency within 14-21 workdays after the fingerprint chart is received by OPM. The NAC and NACI will be completed in approximately 120 calendar days and sent to your agency to close out the investigation.

If the Applicant is a naturalized U.S. citizen, legal permanent resident, legal alien, or presented to the Sponsor any of the identity source documents numbered 2 through 10, from List A of the I-9, a records check should be scheduled with the U.S. Citizenship and Immigration Service (CIS), Department of Homeland Security, by placing an “H” in Block B, Extra Coverage, of the AUO section at the top of the SF-85.

If the Applicant presented to the Sponsor documents 5 or 7 from List B of the Attachment as a source identity document, schedule a check of U.S. Military Personnel Records (MILR) by placing a “G” in Block B, Extra Coverage.

Finally, if any discrepancies in date or place of birth for U.S. born Applicants are discovered, schedule a Bureau of Vital Statistics (BVS) check by placing an “L” in Block B, Extra Coverage placing a “2” in Block B. This check may be scheduled as part of the NACI or separately through use of OPM’s Special Agreement Check (SAC). USDA Human Resources Directors (HR Directors) were previously provided SAC completion procedures.

Refer to OPM’s publication IS-15, Requesting OPM Personnel Investigations, and U.S. Department of Agriculture Personnel Security Bulletin No. 06-01, Subject: Advance FBI Fingerprint Checks for Issuing Personal Identity Verification (PIV) I.D. Badges under HSPD-12, dated November 1, 2005 (see [www.usda.gov/dalpd/d/bulletins.htm](http://www.usda.gov/dalpd/d/bulletins.htm)). The IS-15 has detailed instructions on coding the AUO block as well as information on fingerprinting, what documents are needed for an NACI (see chart on page 6), instructions on the limited questions (items 1,2, 8 through 13, 16 and 17a) that contractors must answer when completing the OF-306, and a variety of other useful information. The Personnel Security Bulletin No. 06-01 contains instructions on scheduling advance FBI fingerprint checks.



OPM's SF-85 and OF-306 Accept Guidelines explain what must be shown in each block to ensure proper form completion for forms SF-85 and OF-306. If one of these forms is not properly coded, the Sponsor photocopies and returns the form(s). If the SF-85 and/or OF-306 are not properly completed, photocopy and return the form(s) to the Sponsor. USDA's Personnel and Document Security Division's (PDSD) internal checklist can be used as a transmittal memo to inform the Sponsor what corrections are needed. Agencies should modify the checklist to suit their needs.

Prior to scheduling the NACI, contractors and affiliates should be asked if they have a previous NACI. If contractors state a previous NACI was completed, the contractor shall be advised to contact the contracting companies' human resources or security offices and request the record be faxed directly to the USDA contracting officer's representative or other authorized Federal official.

It is an agency management decision who schedules and adjudicates NACIs for agency contractors or affiliates.

Providing LincPasses to non-employee affiliates (hereafter, "affiliates") such as volunteers, gratuitous employees, collaborators, state and local government employees, and others carrying out the work of the Secretary of Agriculture is discretionary with USDA agencies. It depends on the level of access the affiliate requires to federally controlled facilities or information systems.

Authority to conduct NACIs on affiliates is found at 5 CFR 736.10 1.

Agencies should note that the legal instruments under which affiliates work, e.g., volunteer, cooperative, and memoranda of understanding, and similar instruments will most likely require modification before LincPass credentials can be authorized. Advice from the agency office responsible for such agreements is recommended prior to requiring completion of the forms needed to conduct a NACI.

OMB deadlines for verifying and/or completing NACIs:

- Verify and/or complete NACIs for all current employees with less than 15 years of Federal service: No later than October 27, 2007.
- Verify and/or complete NACIs for all current contractors: No later than October 27, 2007.
- Verify and/or complete NACIs for all current employees with more than 15 years of Federal service: No later than October 27, 2008.

Federal employees transferring to USDA will require a favorably adjudicated Federal background investigation. The Sponsor will check with the Applicant's former department or agency to verify he/she was issued a valid LincPass.

If an applicant needs a national security clearance or a certificate to hold a public trust position, he/she will be asked to complete either a SF-86, Questionnaire for National Security Positions, or SF-85P, Questionnaire for Public Trust Positions, and a more in-depth background investigation will be scheduled with OPM through the PDSD.



USDA agency adjudicators and their supervisors are the only individuals authorized to see NACI results. USDA Department-level personnel security specialists and their supervisors will see the background investigation results if, in addition to the LincPass, the position requires a national security clearance or public trust suitability determination.

An applicant can see his/her NACI by sending a signed and dated written request to OPM-IS, FOIP, Post Office Box 618, Boyers, PA 16018-0618, or fax to OPM-IS, FOIP at (724) 794-4590. The applicant must include his/her full name, social security number, date and place of birth.

DRAFT

## Section 7 Adjudication

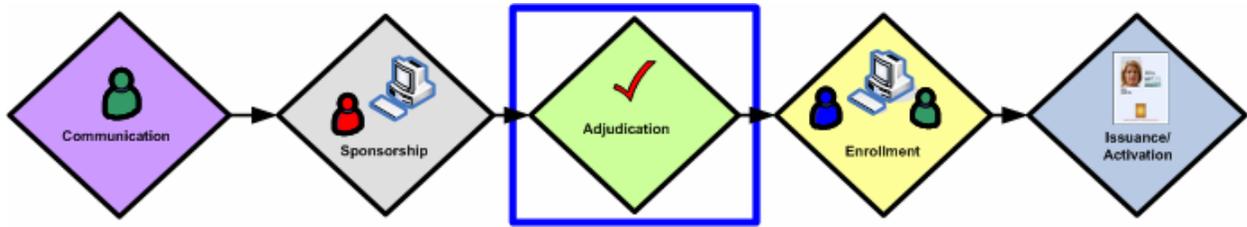


Figure 33: Adjudication Overview

After an applicant is sponsored and has enrolled in-person at an enrollment workstation, a completed enrollment package is submitted for adjudication. The required background checks for a LincPass include a U.S. Federal Bureau of Investigation (FBI) check and National Agency Check with Inquiries (NACI). It is the responsibility of the Adjudicator at the agency to review and approve or reject the results of the background investigations. Each agency's Adjudicator using Payroll Personnel will enter the Adjudicator portal of the USAccess website. Agencies in EmpowHR input the data directly into the Employee's record. The Adjudicator provides a decision that will be recorded as part of the applicant's enrollment record. The Adjudicator provides an "approve" or "reject" decision in the system.

Once an Adjudicator is ready to record a decision for an applicant in the system based on the BI information reviewed, the Adjudicator must enter the Adjudicator portal and indicate that decision. This decision is included in the applicant's enrollment record. In order to perform this function, the Federal employee designated as the Adjudicator accesses the GSA HSPD-12 Shared Service Solution website, enters the Adjudicator portal using his/her secure login credentials, reviews each individual applicant profile in the adjudication queue, and makes the "approve" or "reject" decision. If the applicant's background check is approved, the Adjudicator is responsible for sending the notification to print the card. The Adjudicator performs this by approving the results of the check and clicking the submit button.

All Adjudicators are required to enroll and obtain a PIV prior to conducting any Adjudicator duties and must complete online Adjudicator training. Once completed, the Agency Adjudicator may begin performing Adjudicator duties.

The Adjudicator should click on the Applicant ID of the person whose record he/she chooses to review and record a result. Clicking on the Applicant ID pulls up that Applicant's profile. The Applicant Profile page displays the status of each of the background check results as either "Pending," "Approved," or "Rejected." Those checks in "Pending" status require action by the Adjudicator. If either the FBI Response or the NACI response is approved, and the respective other check remains pending, a card is printed for the applicant. The Adjudicator has the option to enter comments prior to clicking the "Submit" button.

## **7.1 New Adjudication Record**

After an Applicant is sponsored and has enrolled in person at an enrollment station, a completed enrollment package is submitted for adjudication. The required background checks for a LincPass include a U.S. Federal Bureau of Investigation (FBI) check and a National Agency Check with Inquiries (NACI). It is the responsibility of the HSPD-12 Adjudicator at the agency to review and approve or reject the results of the background investigations

## **7.2 Adjudication Workflows in EmpowHR**

### **7.2.1 Fingerprint Adjudication in EmpowHR**

The following diagram details the workflow of fingerprint adjudication of an applicant by the Adjudicator and Sponsor in the EmpowHR system.

DRAFT

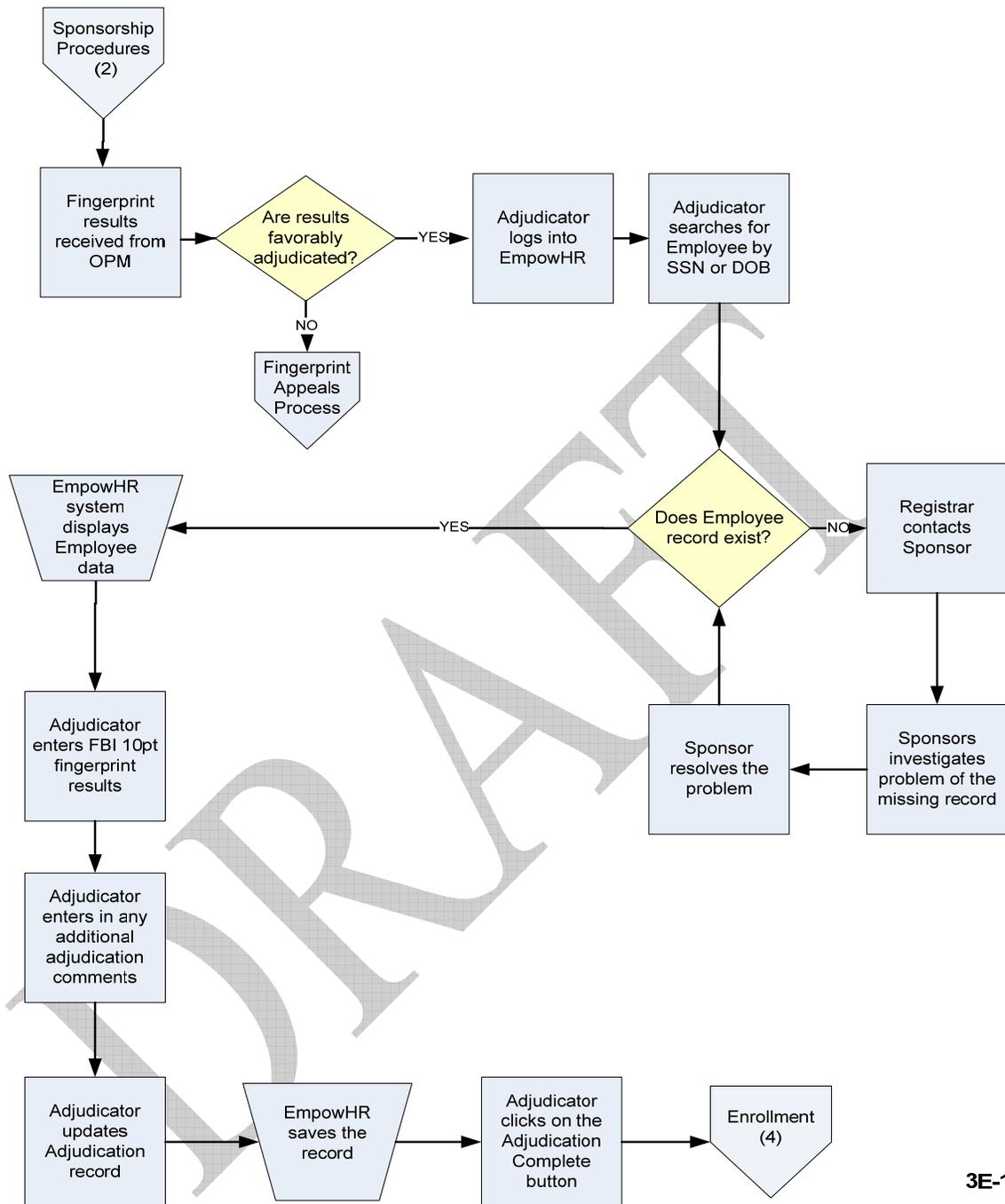


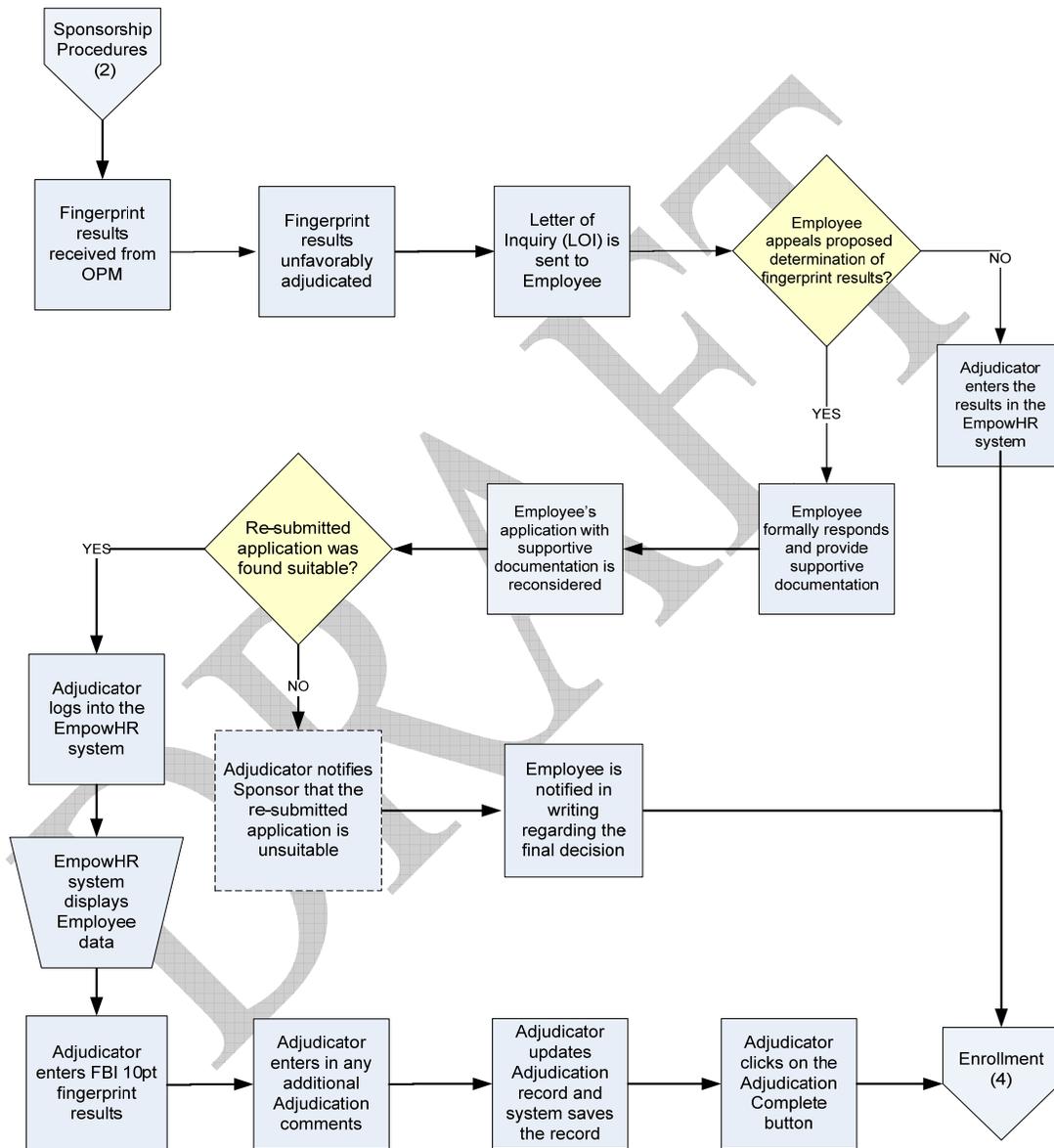
Figure 34: Fingerprint Adjudication in EmpowHR (3E-1)

1. The fingerprint results are received from OPM.
2. The fingerprint results are reviewed and deemed either favorable or not favorable. If fingerprint results are not favorable then an appeal process may be initiated.

3. If fingerprint results are favorable, the Adjudicator searches for the Applicant in the system by SSN or DOB to determine if they are a new or existing employee. The system displays the Applicant's Adjudication record. The initial record should show "pending" for both FBI/NAC and NACI/Higher results.
4. If Applicant's Adjudication record can not be found in the system, the Registrar contacts the Sponsor to investigate and resolve the problem.
5. The Adjudicator enters the FBI/NAC Adjudication results. The default value is "pending" and the possible updates are either "approved" or "rejected". A rejection result will automatically terminate the LincPass or will prevent a LincPass from being printed.
  - a. The Adjudicator enters the FBI/NAC start date and end date.
6. The Adjudicator enters the NACI/Higher Adjudication results. The default value is "pending" and the possible updates are either "approved" or "rejected". A rejection result will automatically terminate the LincPass or will prevent a LincPass from being printed.
  - a. The Adjudicator enters the FBI/NAC start date and end date.
7. The Adjudicator enters comments regarding the Applicant's Adjudication if necessary.
8. The Adjudicator clicks on the "update" button. The system automatically dates and saves the Adjudication record.
9. The system requests confirmation that Adjudication is complete.
10. The Adjudicator clicks on the "Adjudication Complete" button, which triggers a card issuance request to the system to prepare a card production file to be sent to the card production facility.

### 7.2.2 Fingerprint Adjudication Appeals Process in EmpowHR

The following diagram details the workflow of the appeal of fingerprint adjudication results in the EmpowHR system.



3E-1a

Figure 35: Fingerprint Appeal Process in EmpowHR (3E-1a)

1. Fingerprint (FP) results received from OPM and reviewed by the Adjudicator.
2. The FP results are unfavorably adjudicated.
3. The Adjudicator sends the Employee a Letter of Inquiry (LOI) requesting facts and circumstances surrounding FP results.
4. The Employee may or may not choose to respond to the LOI in writing and initiate the FP appeal process.
5. If the Employee chooses to officially respond to the LOI, then the Adjudicator follows their agency-specific FP appeal process.
6. If the Employee chooses not to respond to the LOI, then the Adjudicator enters the FP results into the EmpowHR system.
7. Employee re-submits the application with supportive documentation to be reviewed and reconsidered.
8. If the re-submitted application is found suitable than the adjudication process continues.
9. If the re-submitted application is found un-suitable than the Employee is notified regarding the final decision.
10. Upon successful appeal, the Adjudicator logs into the EmpowHR Web Portal.
11. The Adjudicator searches for the Employee in the system by SSN or DOB to determine if they are a new or existing employee. The system displays the Employee's Adjudication record.
12. The Adjudicator enters the NACI/Higher Adjudication results. The default value is "pending" and the possible updates are either "approved" or "rejected". A rejection result will automatically terminate the LincPass or will prevent a LincPass from being printed.
13. The Adjudicator enters comments regarding the Employee's Adjudication if necessary.
14. The Adjudicator clicks on the "update" button. The system automatically dates and saves the Adjudication record.
15. The system requests confirmation that Adjudication is complete.
16. The Adjudicator clicks on the "Adjudication Complete" button, which triggers a card issuance request to the system to prepare a card production file to be sent to the card production facility.

### 7.2.3 Background Investigation (BI) Process in EmpowHR

The following diagram details the workflow of the background investigation adjudication of an application by the Adjudicator and Sponsor in the EmpowHR system.

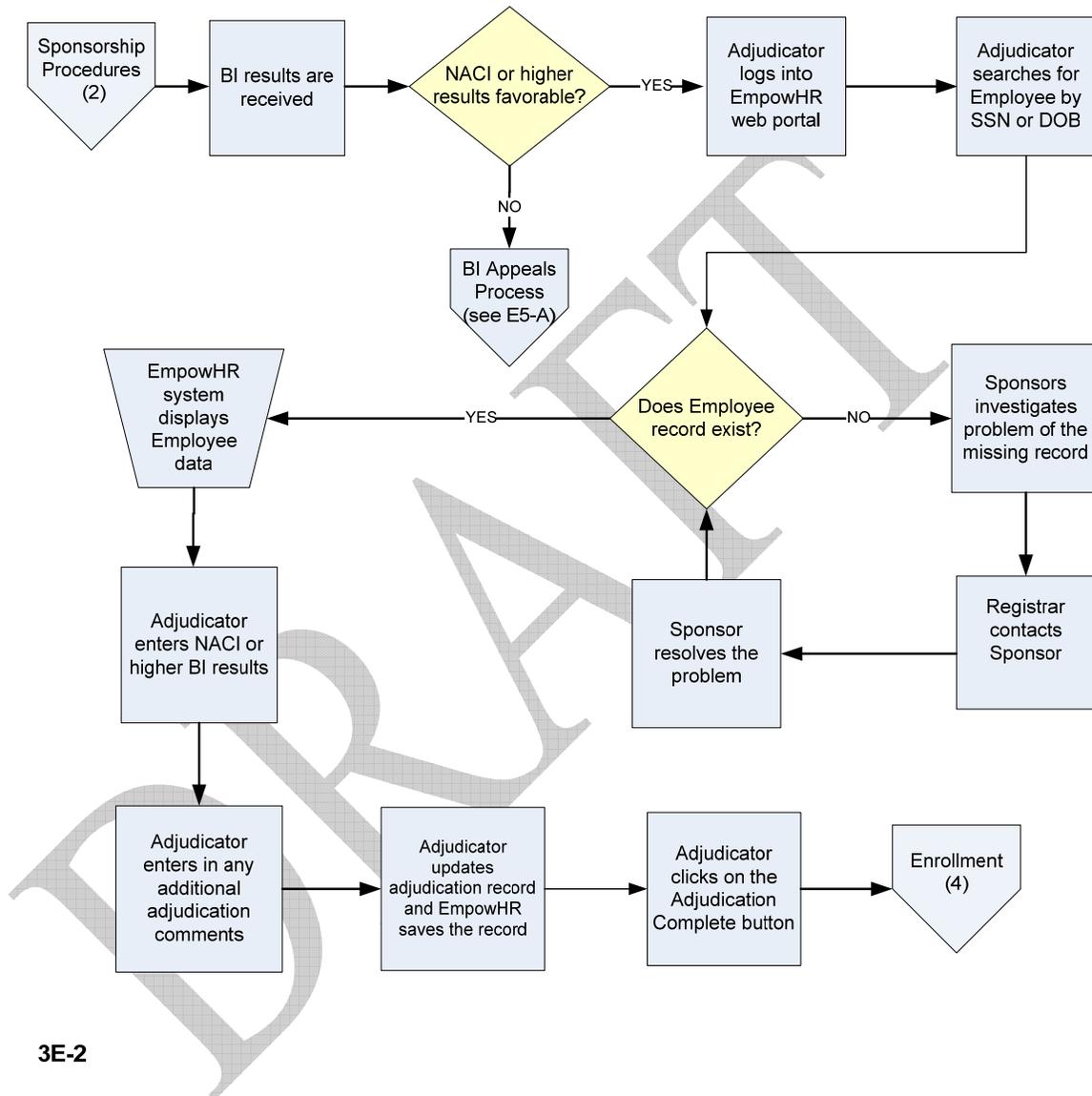


Figure 36: Background Investigation in EmpowHR (3E-2)

1. Background Investigation results received and reviewed by the Adjudicator.
2. If the NACI results are favorable then the Adjudicator enters the NACI/Higher Adjudication results. The default value is “pending” and the possible updates are either “approved” or “rejected”. A rejection result will automatically terminate the LincPass or will prevent a LincPass from being printed.

3. The BI results are reviewed and deemed either favorable or not favorable. If the BI results are not favorable then an appeal process may be initiated. The Adjudicator enters the FBI/NAC start date and end date.
4. The Adjudicator logs into the EmpowHR Web Portal.
5. The Adjudicator searches for the Employee in the system by SSN or DOB to determine if they are a new or existing Employee. The system displays the Employee's Adjudication record. The initial record should show "pending" for both FBI/NAC and NACI/Higher results.
6. If Employee's Adjudication record can not be found in the system, the Registrar contacts the Sponsor to investigate and resolve the problem.
7. The EmpowHR system displays the Employee's data.
8. The Adjudicator enters in comments regarding the Employee's Adjudication if necessary.
9. The Adjudicator clicks on the "update" button. The system automatically dates and saves the Adjudication record.
10. The system requests confirmation that Adjudication is complete.
11. The Adjudicator clicks on the "Adjudication Complete" button, which triggers a card issuance request to the system to prepare a card production file to be sent to the card production facility.

DRAFT

### 7.2.4 Background Investigation Appeals Process in EmpowHR

The following diagram details the workflow of the appeal process of background investigation adjudication results in the EmpowHR system.

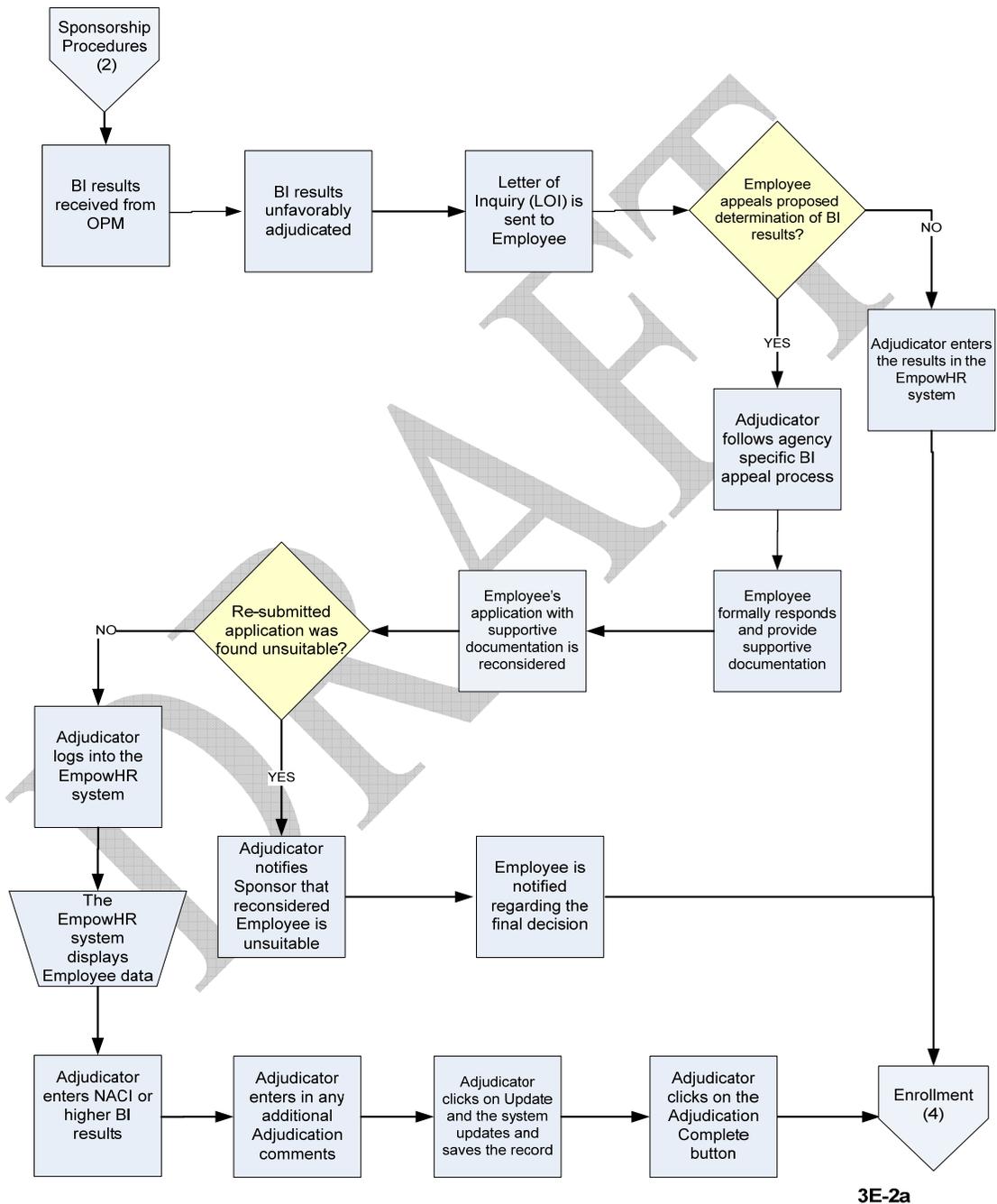


Figure 37: Background Investigation Appeals Process in EmpowHR (3E-2a)

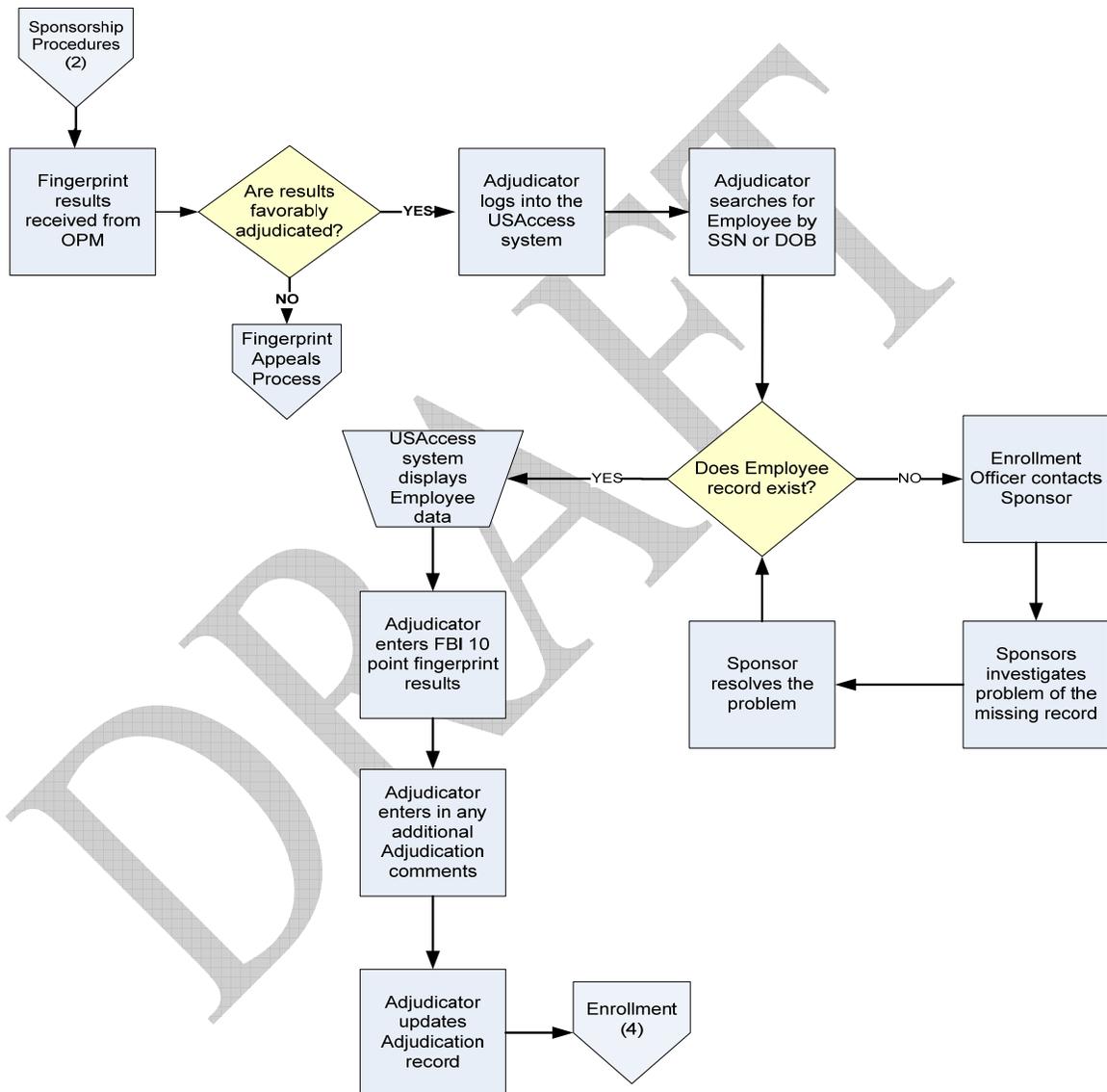


1. Background Investigation (BI) results received from OPM and reviewed by the Adjudicator.
2. The BI results are unfavorably adjudicated.
3. The Adjudicator sends the Applicant a Letter of Inquiry (LOI) requesting facts and circumstances surrounding BI results.
4. The Applicant may or may not choose to respond to the LOI in writing and initiate the BI appeal process.
5. If the Employee chooses to officially respond to the LOI, then the Adjudicator follows their agency-specific BI appeal process.
6. If the Employee chooses not to respond to the LOI, then the Adjudicator enters the BI results into the EmpowHR system.
7. Applicant re-submits the application with supportive documentation to be reviewed and reconsidered.
8. If the re-submitted application is found suitable than the adjudication process continues.
9. If the re-submitted application is found un-suitable than the Employee is notified regarding the final decision.
10. Upon successful appeal, the Adjudicator logs into the EmpowHR Web Portal.
11. The Adjudicator searches for the Employee in the system by SSN or DOB to determine if they are a new or existing employee. The system displays the Employee's Adjudication record.
12. The Adjudicator enters the NACI/Higher Adjudication results. The default value is "pending" and the possible updates are either "approved" or "rejected". A rejection result will automatically terminate the LincPass or will prevent a LincPass from being printed.
13. The Adjudicator enters comments regarding the Employee's Adjudication if necessary.
14. The Adjudicator clicks on the "update" button. The system automatically dates and saves the Adjudication record.
15. The system requests confirmation that Adjudication is complete.
16. The Adjudicator clicks on the "Adjudication Complete" button, which triggers a card issuance request to the system to prepare a card production file to be sent to the card production facility.

### 7.3 Adjudication Workflows in Payroll Personnel

#### 7.3.1 Fingerprint Adjudication Process

The following diagram details the workflow of fingerprint adjudication of an applicant by the Adjudicator and Sponsor in the Payroll Personnel system.



3P-1

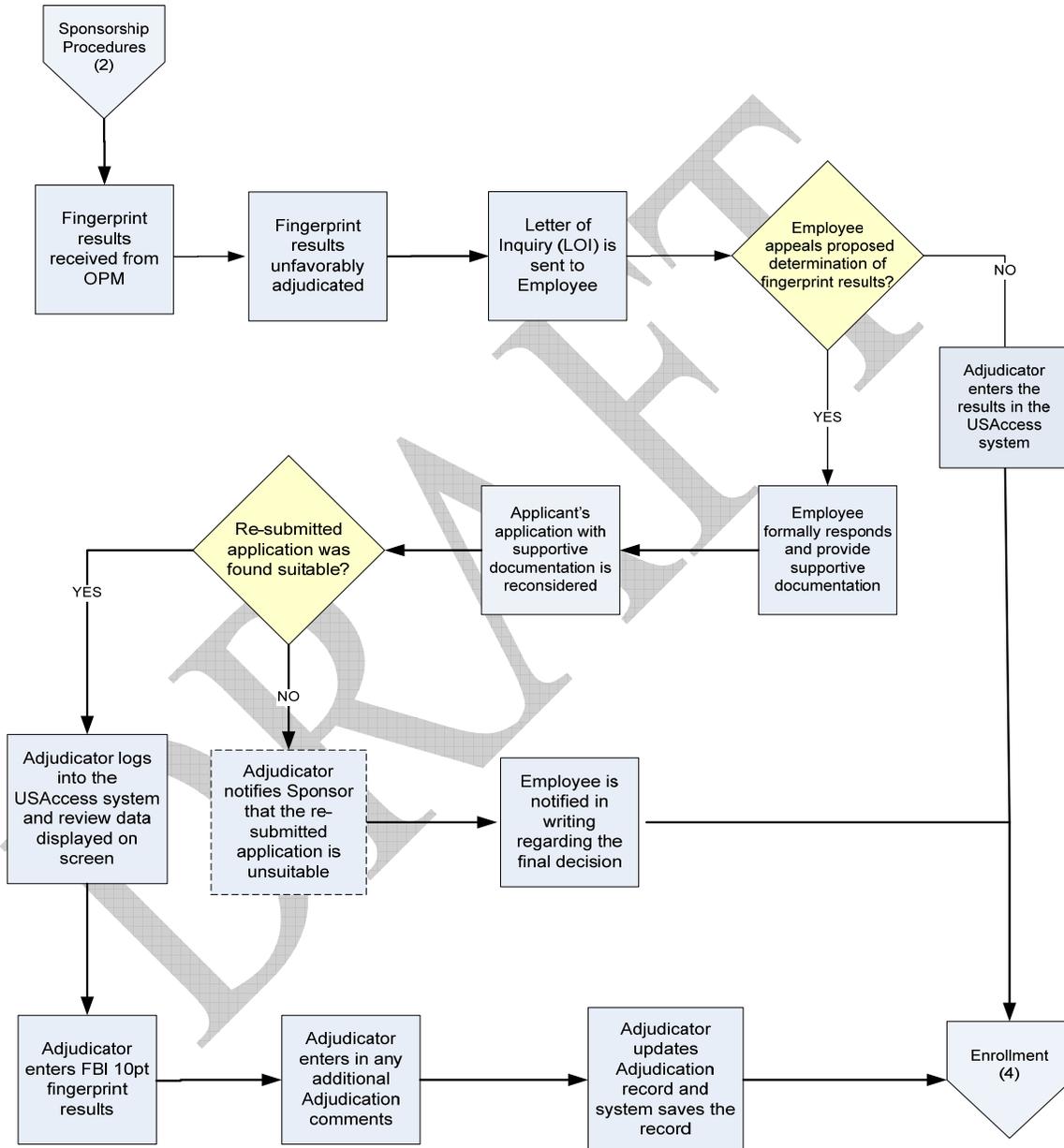
Figure 38: Fingerprint Adjudication in Payroll Personnel (3P-1)



1. The fingerprint results are received from OPM.
2. The fingerprint results are reviewed and deemed either favorable or not favorable. If the results are not favorable then an appeal process may be initiated.
3. If fingerprint results are favorable, the Adjudicator searches for the Employee in the USAccess System by SSN or DOB to determine if they are a new or existing employee. The system displays the Employee's Adjudication record. The initial record should show "pending" for both FBI/NAC and NACI/Higher results.
4. If Employee's Adjudication record can not be found in the system, the Registrar contacts the Sponsor to investigate and resolve the problem.
5. The Adjudicator enters the NACI/Higher Adjudication results. The default value is "pending" and the possible updates are either "approved" or "rejected". A rejection result will automatically terminate the LincPass or will prevent a LincPass from being printed.
6. The Adjudicator enters comments regarding the Employee's Adjudication if necessary.
7. The Adjudicator clicks on the "update" button. The USAccess System automatically dates and saves the Adjudication record.
8. The USAccess System requests confirmation that Adjudication is complete.
9. The Adjudicator clicks on the "Adjudication Complete" button, which triggers a card issuance request to the system to prepare a card production file to be sent to the card production facility.

### 7.3.2 Fingerprint Appeal Adjudication Process

The following diagram details the workflow of the appeal of fingerprint adjudication results in the Payroll Personnel system.



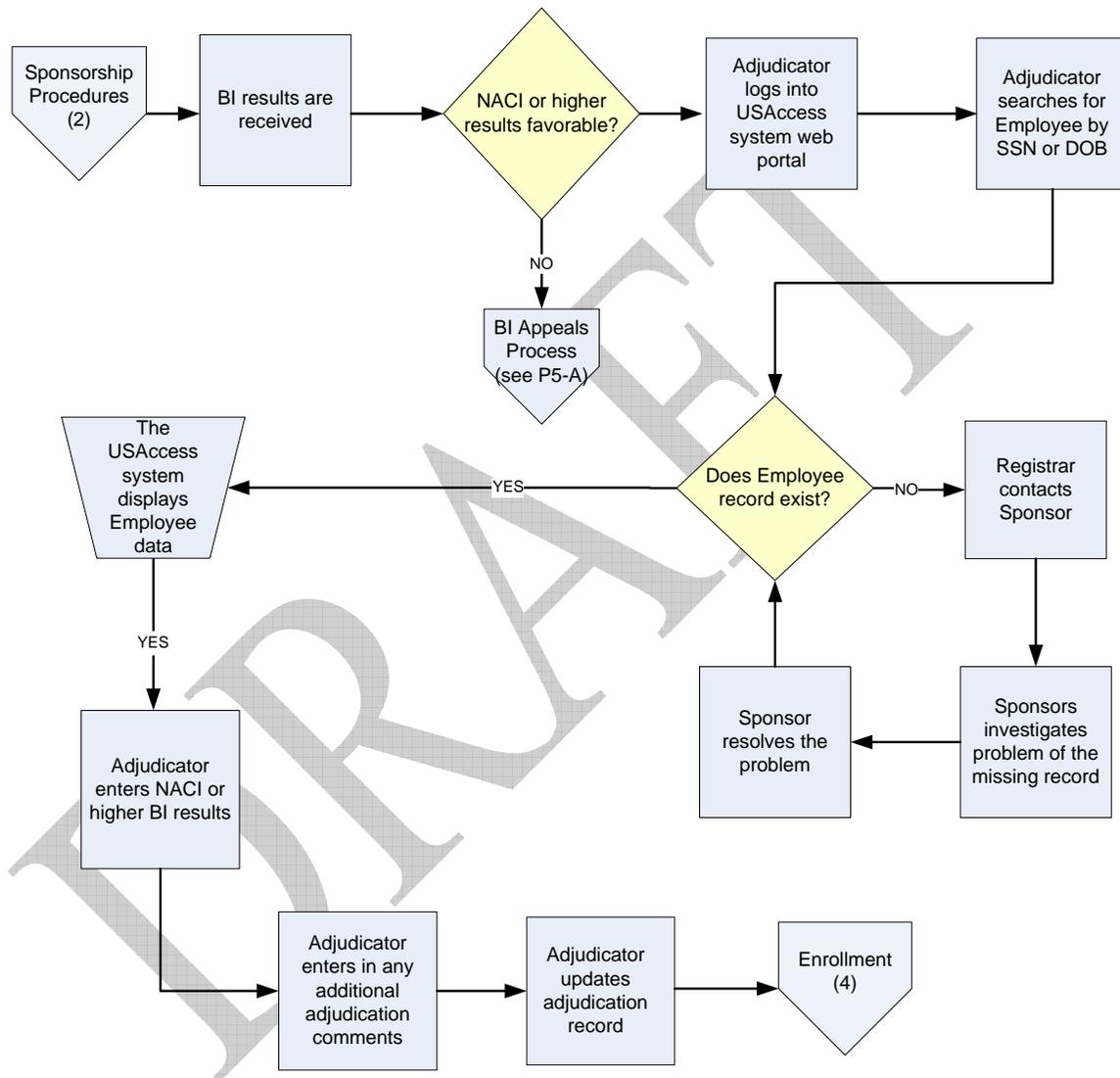
3P-1a

Figure 39: Fingerprint Appeal Adjudication Process in Payroll Personnel (3P-1a)

1. Fingerprint (FP) results received from OPM and reviewed by the Adjudicator.
2. The FP results are unfavorably adjudicated.
3. The Adjudicator sends the Employee a Letter of Inquiry (LOI) requesting facts and circumstances surrounding FP results.
4. The Employee may or may not choose to respond to the LOI in writing and initiate the FP appeal process.
5. If the Employee chooses to officially respond to the LOI, then the Adjudicator follows their agency-specific FP appeal process.
6. If the Employee chooses not to respond to the LOI, then the Adjudicator enters the FP results into the USAccess System.
7. Employee re-submits the application with supportive documentation to be reviewed and reconsidered.
8. If the re-submitted application is found suitable than the adjudication process continues.
9. If the re-submitted application is found un-suitable than the Employee is notified regarding the final decision.
10. Upon successful appeal, the Adjudicator logs into the USAccess Web Portal.
11. The Adjudicator searches for the Employee in the system by SSN or DOB to determine if they are a new or existing employee. The system displays the Employee's Adjudication record.
12. The Adjudicator enters the NACI/Higher Adjudication results. The default value is "pending" and the possible updates are either "approved" or "rejected". A rejection result will automatically terminate the LincPass or will prevent a LincPass from being printed.
13. The Adjudicator enters comments regarding the Employee's Adjudication if necessary.
14. The Adjudicator clicks on the "update" button. The USAccess System automatically dates and saves the Adjudication record.
15. The system requests confirmation that Adjudication is complete.
16. The Adjudicator clicks on the "Adjudication Complete" button, which triggers a card issuance request to the system to prepare a card production file to be sent to the card production facility.

### 7.3.3 Background Investigation Adjudication Process in Payroll Personnel

The following diagram details the workflow of the background investigation adjudication of an application by the Adjudicator and Sponsor in the Payroll Personnel system.



3P-2

**Figure 40:** Background Investigation Adjudication Process in Payroll Personnel (3P-2)

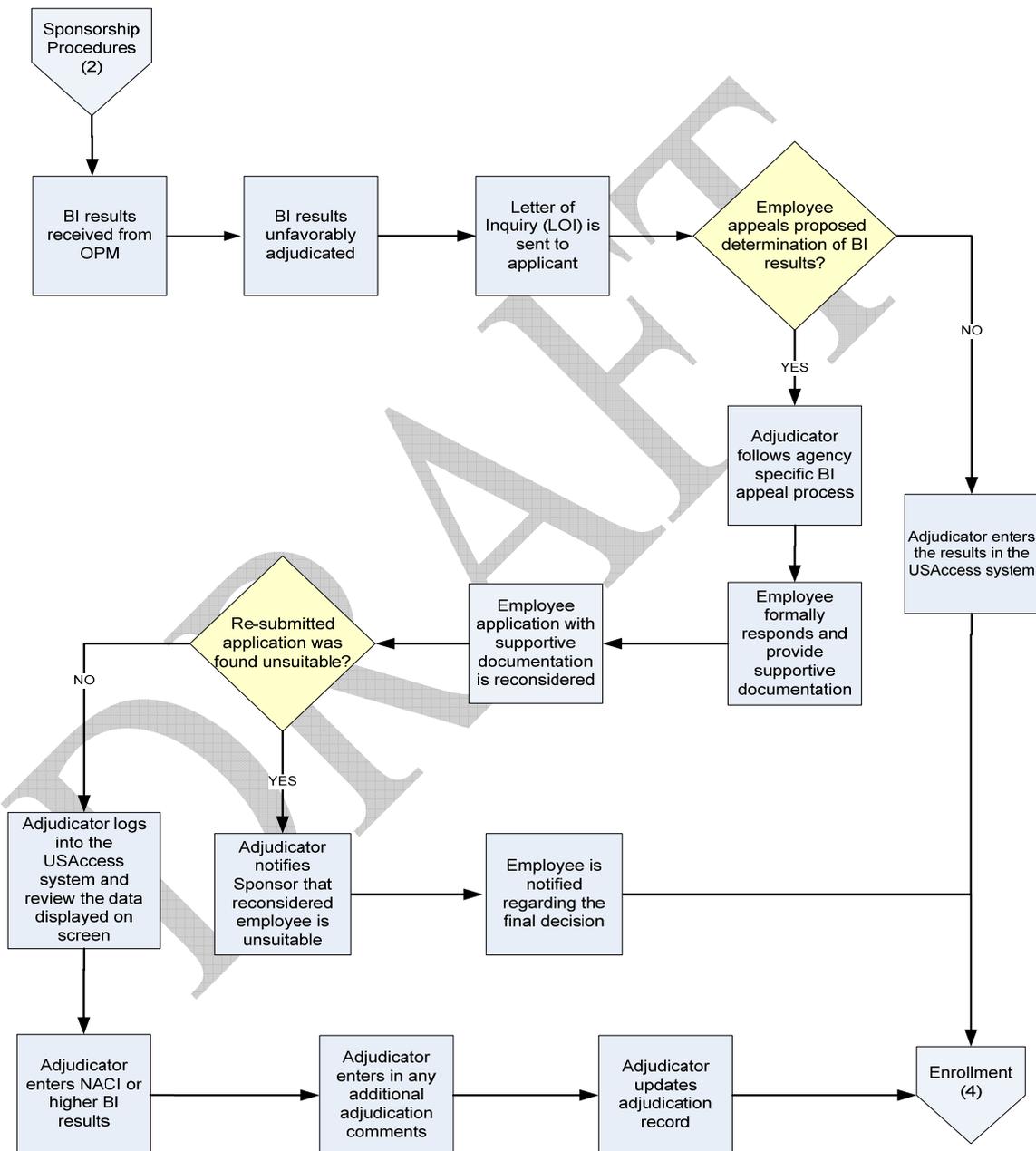
1. Background Investigation results received and reviewed by the Adjudicator.
2. The BI results are reviewed and deemed either favorable or not favorable. If the BI results are not favorable then an appeal process may be initiated.

3. If the NACI results are favorable then the Adjudicator enters the NACI/Higher Adjudication results. The default value is “pending” and the possible updates are either “approved” or “rejected”. A rejection result will automatically terminate the LincPass or will prevent a LincPass from being printed. The Adjudicator enters the FBI/NAC start date and end date.
4. The Adjudicator logs into the USAccess Web Portal.
5. The Adjudicator searches for the Employee in the system by SSN or DOB to determine if they are a new or existing Employee. The system displays the Applicant’s Adjudication record. The initial record should show “pending” for both FBI/NAC and NACI/Higher results.
6. If Employee’s Adjudication record can not be found in the system, the Registrar contacts the Sponsor to investigate and resolve the problem.
7. The USAccess System displays the applicants’ data.
8. The Adjudicator enters comments regarding the Employee’s Adjudication if necessary.
9. The Adjudicator clicks on the “update” button. The system automatically dates and saves the Adjudication record.
10. The system requests confirmation that Adjudication is complete.
11. The Adjudicator clicks on the “Adjudication Complete” button, which triggers a card issuance request to the system to prepare a card production file to be sent to the card production facility.

DRAFT

### 7.3.4 Background Investigation Appeals Adjudication Process in Payroll Personnel

The following diagram details the workflow of the appeal process of background investigation adjudication results in the Payroll Personnel system.



3P-2a

Figure 41: Background Investigation Appeals Adjudication Process (3P-2a)

1. Background Investigation (BI) results received from OPM and reviewed by the Adjudicator.
2. The BI results are unfavorably adjudicated.
3. The Adjudicator sends the Employee a Letter of Inquiry (LOI) requesting facts and circumstances surrounding BI results.
4. The Employee may or may not choose to respond to the LOI in writing and initiate the BI appeal process.
5. If the Employee chooses to officially respond to the LOI, then the Adjudicator follows their agency-specific BI appeal process.
6. If the Employee chooses not to respond to the LOI, then the Adjudicator enters the BI results into the USAccess System.
7. Employee re-submits the application with supportive documentation to be reviewed and reconsidered.
8. If the re-submitted application is found suitable than the adjudication process continues.
9. If the re-submitted application is found un-suitable than the Employee is notified regarding the final decision.
10. Upon successful appeal, the Adjudicator logs into the USAccess Web Portal.
11. The Adjudicator searches for the Employee in the system by SSN or DOB to determine if they are a new or existing employee. The system displays the Employee's Adjudication record.
12. The Adjudicator enters the NACI/Higher Adjudication results. The default value is "pending" and the possible updates are either "approved" or "rejected". A rejection result will automatically terminate the LincPass or will prevent a LincPass from being printed.
13. The Adjudicator enters comments regarding the Employee's Adjudication if necessary.
14. The Adjudicator clicks on the "update" button. The system automatically dates and saves the Adjudication record.

## **Section 8 Adjudication Policies**

### **8.1 Change to Adjudication Record Status**

As part of the adjudication the different scenarios for changing the record status in EmpowHR are the following. The scenarios are the same for entering or loading a legacy adjudication records in batch mode prior to enrollment.

- FBI Fingerprint Check Approved and NACI Investigation Pending
- FBI Fingerprint Check Rejected and NACI Investigation Pending
- FBI Fingerprint Check Pending and NACI Investigation Approved
- FBI Fingerprint Check Pending and NACI Investigation Rejected
- FBI Fingerprint Check Approved and NACI Investigation Rejected
- FBI Fingerprint Check Approved and NACI Investigation Approved

### **8.2 Adjudicator Responsibilities**

Agency adjudicators are individuals responsible for adjudicating NACI results for new and current federal employees and contractors holding non-Sensitive Positions, determining an Applicant's eligibility for a LincPass, and when required, proposing denial or revocation of that Card. PDSD Adjudicators will adjudicate other types of investigations and notify the agency of results.

### **8.3 Adjudicator Training**

The USDA Graduate School offers a 3-day class on suitability adjudications and it is the only OPM accredited course on Suitability Adjudications. This course is presented in major cities across the U.S. and costs \$795.00. In addition USAccess will provide training to those Adjudicators who will need access to the USAccess HSPD-12 system.

HR Directors will use the following documents in electronic format to assist with agency HSPD-12 adjudications:

- USDA Personnel and Document Security Division (PDSD) Letter of Inquiry Template (LOI). (See [Appendix B](#))
- USDA PDSD Adjudication Worksheet Template (Worksheet reduces adjudication time for issue cases.) (See [Appendix B](#))
- USDA PDSD case papers for a mock PIV ID Card denial.

### **8.3.1 Verification of Contractor NACIs**

Prior to scheduling the NACI, contractors should be asked if they have a previous Federal Background Investigation. If contractors state a previous investigation was completed, the contractor shall be advised to contact the contracting company's human resources or security offices and request a record of the favorably adjudicated investigation be faxed directly to the USDA contracting officer's representative or other authorized Federal official. However, if a contractor has had a break in service of more than two years from employment under a Federal contract, then he/she will need another NACI.

USDA agency adjudicators and their supervisors are the only individuals authorized to see an applicant's NACI results. PDSO personnel security specialists and their supervisors will have access to the applicant's background investigation results if, in addition to the LincPass the applicant's position requires a national security clearance or public trust suitability determination.

### **8.3.2 Adjudication of NACI Records Checks**

Results of records checks with the U.S. Citizenship and Naturalization Service, State Bureaus of Vital Statistics, U.S. Military Personnel Records, and similar identity record checks should be compared against the identity information provided by the Applicant.

Personal identity information (names and addresses used) is reviewed if contained in the results of a records check. Any identified names and addresses are compared to the names and addresses provided by the Applicant on the SF-85, Questionnaire for Non-Sensitive Positions. If name(s) or address(es) are shown in the results of a records check, but are not listed on the SF-85 and should have been listed, a LOI is sent to the Applicant asking if he or she has any knowledge of the undisclosed names/addresses. LOIs should be used if the difference in names is significant, e.g., the names used are not common variations of the Applicant's proper name. For example, if the Applicant's proper first name is "Raymond," but "Ray" is listed in the results of a records check, a LOI is not usually needed. However, if the proper first name is "Raymond," but "Richard" is shown on the record check results, a LOI is needed. Adjudicators must use sound judgment when resolving name issues.

The response to the LOI is carefully analyzed to determine credibility. If there are remaining doubts regarding the Applicant's identity the Adjudicator will need to resolve that doubt before proceeding. An OPM Reimbursable Suitability/Security Investigation (RSI) or other form of agency inquiry may be needed in some cases. RSI's are focused investigations that provide information to resolve issues developed about an individual. An RSI may be used to resolve identity issues. An OPM Special Interview (SPIN) may be requested as part of the RSI. Agencies may obtain a sworn affidavit from the Applicant as part of the SPIN.

If Applicants state that the name/address differences were caused by identity theft, the applicants will be asked to provide documentation confirming the identity theft. Applicants will send copies of letters they sent or are sending to the U.S. Federal Trade Commission, credit bureaus, and other organizations to report the theft of their identities.

Each situation will differ in resolving disqualifying information discovered during the adjudication process. If the Applicant has not already provided an explanation of the potentially disqualifying information, the Applicant will be asked to do so in writing. The Applicant's written explanation is considered as well as the factors shown to the extent those factors are applicable. An initial determination will be made and discussed with the Adjudicator's supervisor and the Sponsor. If the determination is unfavorable, the procedures in section 2.4 (c.) of the DM are followed. Authorizing a LincPass in these situations is a risk-based decision requiring the use of sound judgment. If the Applicant is currently under wants, warrants, charges, or indictment for any violations of the law, or is currently on probation or parole, the Applicant and Sponsor are advised that registration cannot proceed until those matters are resolved.

When making a LincPass eligibility determination, the Adjudicator must find whether or not the identity provided to the Sponsor 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:

- Misconduct or negligence in employment
- Criminal or dishonest conduct
- Material, intentional false statement or deception or fraud in examination or appointment
- Refusal to furnish testimony as required by §5.4 of Title 5, C.F.R.
- 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
- Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation
- Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force
- Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question

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:

- The nature of the position for which the person is applying or in which the person is employed
- The nature and seriousness of the conduct

- The circumstances surrounding the conduct
- The recency of the conduct
- The age of the person involved at the time of the conduct
- Contributing societal conditions
- The absence or presence of rehabilitation or efforts toward rehabilitation

## **8.4 Adjudication of FBI Fingerprint Checks**

If fingerprint results reveal an undisclosed felony conviction, Adjudicators should send the Applicant a Letter of Inquiry (LOI) (See [Appendix B](#)) asking for the facts and circumstances surrounding the arrests and convictions, the final disposition of the court charges, and why the conviction was not shown in response to Question 9 of the Applicant's OF-306, Declaration for Federal Employment. In addition, the Adjudicator should contact the court in which the charges were filed and obtain the complaints/statements of charges and the final dispositions when possible. Agencies may also use OPM's Reimbursable Suitability Investigation process or ask the Applicant for copies of documents to resolve such issues. After the facts are gathered and any discrepancies resolved, the adjudication can be completed using the OPM Issue Characterization Chart as guidance, and determine if a material, intentional falsification of the OF-306 occurred.

Calling Applicants to discuss arrest information is not recommended due to possible errors in interpreting or documenting the Applicants' comments.

If an Applicant states that their name/address differences were caused by identity theft, he/she will be asked to provide documentation confirming the identity theft. Applicants should send copies of letters they sent or are sending to the U.S. Federal Trade Commission, credit bureaus, and other organizations to report the theft of their identities.

Only OPM is authorized to conduct background investigations on USDA employees and contractors. Agencies have the authority to send LOIs, obtain court records, and interview Applicants to resolve issues. Once the Applicant begins work for USDA, credible allegations of misconduct are subject to agency misconduct or USDA Office of the Inspector General inquiries or investigations.

## **8.5 Appeal Procedures for Denial or Revocation of Credential**

### **8.5.1 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).

### **8.5.2 Appeal Rights for Contractors and Affiliate Applicants**

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 proposed 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.

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.

Decision - After consideration of the determination and any documentation submitted by the Applicant for reconsideration of the initial 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. The CO will notify the company that the applicant either did not provide his/her true identity or was found unsuitable to work on a USDA contract. Specific details will not be provided to the CO or the company, in an effort to protect the Applicant's privacy. The reconsideration decision will be final.

### **8.5.3 Record Retention**

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

Investigative reports and related documents furnished to agencies by investigative organizations for use in making PIV ID credential eligibility determinations should be destroyed in accordance with the investigating agency instructions.

Appeal records related to unsuccessful adjudications should be destroyed no sooner than 4 years but no later than seven years after final appeal decision. USAccess Records Schedule 1 and 18 at: <http://www.archives.gov/records-mgmt/ardor/records-schedules.html> and DR 3080-01, and DR 3080-001, Records Management, at: <http://www.ocio.usda.gov/directives/doc/DR3080-001.pdf>.

#### 8.5.4 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. With the automation of many processes in PIV-II some of these forms may not be necessary. The following is a list of approved forms for use in the HSPD-12 process:

AD-1197:	PIV-I Request and Issuance Approval Form or OMB-approved equivalent
FD-258:	Fingerprint Chart used to conduct contractor or affiliate FBI fingerprint checks.
OF-306:	Declaration for Federal Employment
OF-612:	Optional Application for Federal Employment
OPM OFI-79A:	Report of Agency Adjudicative Action on OPM Personnel Investigations
Standard Form (SF) 85:	OPM Questionnaire for Non-Sensitive Positions (to be completed using e-QIP when available)
SF 85P:	OPM Questionnaire for Public Trust Positions (to be completed using e-QIP)
SF 86:	OPM Questionnaire for National Security Positions (to be completed using e-QIP)
SF 87:	Fingerprint Chart used to conduct FBI fingerprint checks for federal appointees and employees and applicants for federal employment.

## Section 9 Enrollment Process

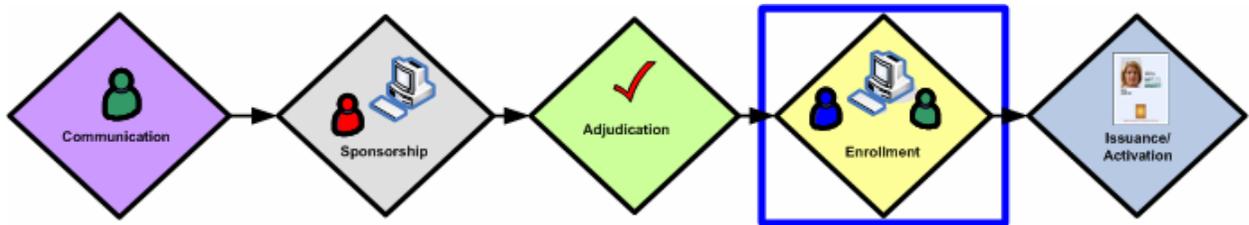


Figure 42: Enrollment Overview

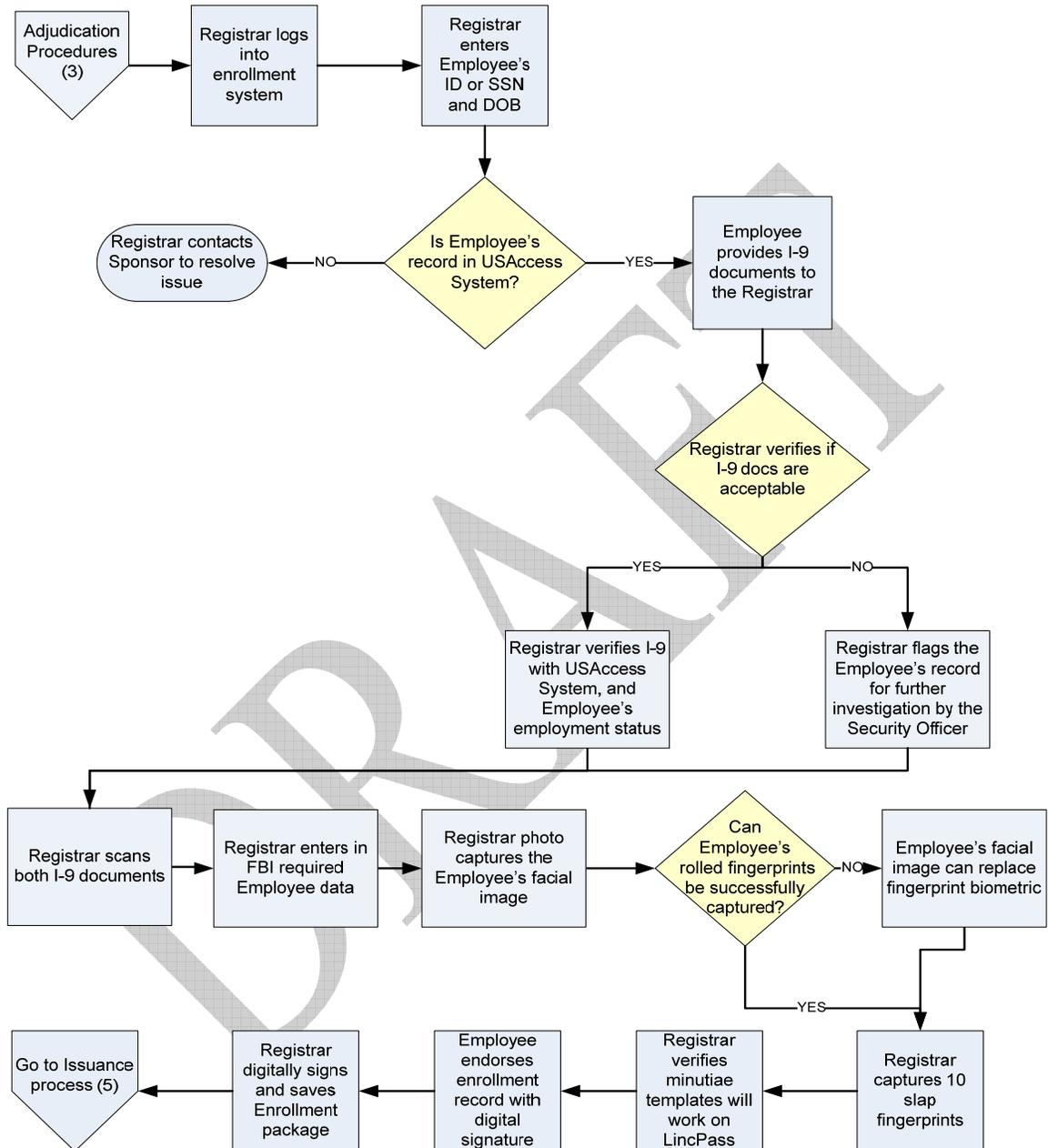
The enrollment process refers to the process of identity-proofing and capturing the applicant's identification information, identity source documents, and biometrics. During enrollment, various types of biometric and source identity information are collected from the applicant and added to their record in USAccess.

### 9.1 New Enrollment

The HSPD-12 Registrar is responsible for verifying the identity of the Applicant, capturing biographic information, a digital photo, biometrics, and documenting any issues encountered during the enrollment process. The applicant is sponsored and put into the USAccess system. The applicant will be notified by e-mail to schedule an appointment to enroll. The applicant schedules an appointment time and location in a web based application. 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. Registrar validates and scans the applicant's two identity source (I-9) documents. 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. Registrar validates all information is correct and complete. Registrar digitally signs Applicant's enrollment file and sends to OPM.

### Detailed Enrollment Workflow

The following diagram details the workflow of the enrollment of an applicant by the Registrar in the USAccess System.



4

Figure 43: Enrollment (4)

1. The Registrar logs in to the enrollment system.
2. The Registrar enters the Applicant ID or SSN and DOB.
3. If the IDMS record is not found the Registrar contacts the Sponsor and stops the process. The Sponsor may investigate the following:
  - a. Is Employee in USAccess System or feeder system (EmpowHR, P/P)?
  - b. Did Registrar search for the correct person?
  - c. Is there a process breakdown in the data feeds?
4. The applicant provides I-9 documents to the Registrar. The Registrar verifies that the source documents meet the list of acceptable I-9 source documents.
5. If the source documents are incorrect the Registrar flags the Applicant's record for further investigation by the Security Officer.
6. The USAccess System displays the applicant record when the Applicant's record is found. The Registrar validates data from the IDMS against the I-9 source documents. The Registrar validates that the applicant is authorized for enrollment and that he/she is an active employee.
7. The Registrar scans both I-9 documents for inclusion into the enrollment record.
8. Registrar enters FBI-required Applicant data.
9. Registrar captures applicant facial image
10. The Registrar scans Applicant rolled fingerprints. If unable to capture finger prints, document the inability to capture the biometric data. In this situation, applicant's facial image capture can replace the fingerprint biometrics.
11. Registrar scans Applicant's 10 slap fingerprints. System will verify rolled fingerprints against 10 slap fingerprints to ensure integrity of fingerprint capture.
12. Registrar shall check the primary and secondary fingerprints against the minutiae to ensure that the templates will work when put on the card.
13. Applicant will endorse the record with a digital signature.
14. Registrar digitally signs and saves enrollment package

## **9.2 Invalid Source Documents**

When the Registrar validates the authenticity of the source documents and has reasons to believe that one or both documents could be falsified, the system has the ability to flag the validity of the source documents. The purpose of the flag is to stop the issuance of the card and to notify the Security Officer that an investigation is required. The enrollment process should not be stopped for this event.

## **9.3 Incorrect Source Documents**

If the applicant presents documents that are not on the I -9 list, the enrollment process is stopped and the applicant is notified that the documents do not meet the required list for enrollment.

## Section 10 Issuance



Figure 44: Issuance Overview

Once an applicant has successfully passed the required security checks, the GSA HSPD-12 Shared Service Solution system automatically and securely transmits a card production file to the card production facility. The card production facility uses this file to produce and personalize the card. Once the credentials have been produced, the card production facility is responsible for quality inspection, securely packaging the cards and shipping them back to the designated activation workstation location via a courier service. The card production facility also sends a message to the card management system (CMS) notifying the CMS of the cards that have been produced.

When one or more of the six pre-issuance criteria as specified in the system requirements section are not met, the system shall prevent the card from being printed. The following six prerequisites need to be met to print the card:

1. The applicant has been approved for a PIV Card (Card is required flag is set to yes)
2. The applicant is sponsored
3. A complete, digitally signed enrollment package exists
4. The applicant has a successful FBI or higher adjudication status
5. Applicant is an active Federal employee, Contractor or Affiliate
6. No impersonation match result from 1:M biometric check

### 10.1 Detailed Issuance Process

The following diagram details the workflow of the card issuance process in the USAccess System. The system flow and the steps described in this section cover the following use cases: (a) Normal Valid Card Issuance Process, (b) Pre-issuance Request with Security Issues (c) Pre-issuance Request with Criteria Issues (d) Invalid Card Printing Check (e) Invalid Address (f) Wrong Cards Shipped to Valid Address and (g) No Applicant Match for a Shipped Card.

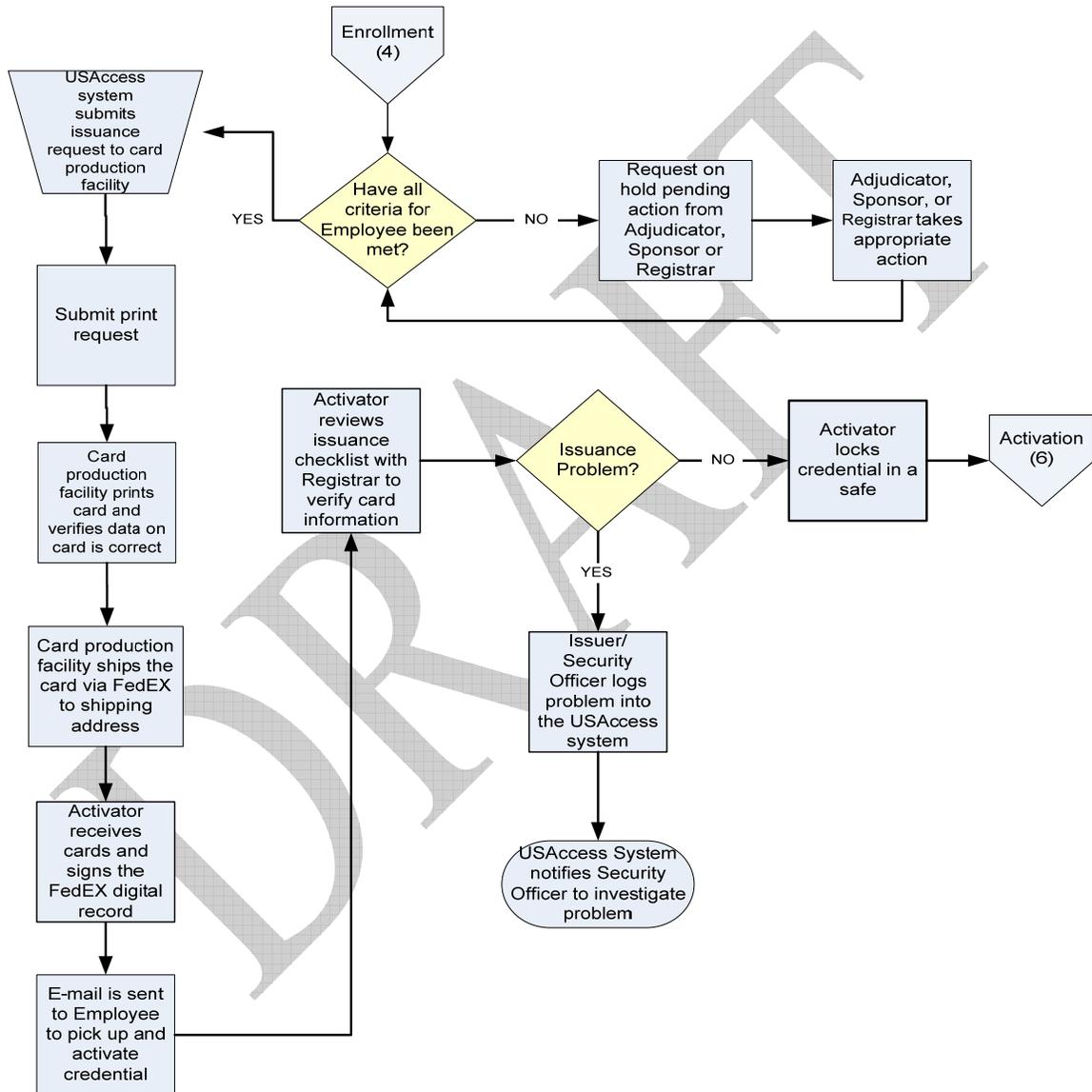


Figure 45: Detailed Issuance Process (5)

1. An approved designation triggers a card issuance request to the system to prepare a card production file to be sent to the card production facility.
2. The following criteria will be met prior to issuing a card:
  - a. The applicant has been approved for a PIV Card (card is required flag is set to yes)
  - b. The applicant is sponsored
  - c. A complete, digitally signed enrollment package exists
  - d. The applicant has a successful FBI or higher adjudication status
  - e. Applicant is an active Federal employee, contractor, or affiliate
  - f. No impersonation matches result from 1 to many biometric checks.
3. The USAccess System creates a pre-issuance package containing all information required to print the card at the centralized printing facility.
4. The USAccess System shall automatically submit the issuance request to the card printing facility.
5. The card is printed and verified to ensure that the data on the card is accurate.
6. The card is shipped via FedEx to the designated location (enrollment station). The shipment will be tracked electronically utilizing the FedEx tracking system.
7. Applicant is notified by email to pick up their LincPass at their designated Enrollment station location.
8. The Activator/Issuer receives the card and reviews the issuance checklist with the Registrar to verify that the correct cards were received.
9. If there is a problem detected during the issuance process the problem is logged into the USAccess System and the security officer is notified to investigate and resolve the problem.
10. If no problem is detected during the issuance process the Activator/Issuer locks the credential in a safe until pick up by the applicant.

## **10.2 Invalid Card Printing Check**

Any anomalies identified during inspection of the post printing record and the pre-issuance request record shall be alerted to the security officer. If this event occurs the system shall flag the issue and prevent the card from being activated. Cards that meet this condition shall be retrieved by the security officer and shall be destroyed. The security officer may request a reprint of the credential, this is the only time that a reprint is authorized.

## **10.3 Wrong Cards Shipped to Valid Address**

If the wrong cards are shipped to a valid address, the cards will be locked up in a secured location and a notification shall be sent to the Security Officer. The Security Officer will be responsible for investigating and correcting the shipping address. The exact details of this procedure are to be determined.

#### ***10.4 No Applicant Match for a Shipped Card***

The possibility exists that the applicant left employment abruptly, leaving a card unclaimed. The Activator/Issuer or Issuer/Activator notifies the Security Officer of this event and sends the PIV card to the Security Officer for destruction. The exact details of this procedure are to be determined.

DRAFT

## Section 11 Activation



Figure 46: Activation Overview

### 11.1 Unattended Activation Workflow

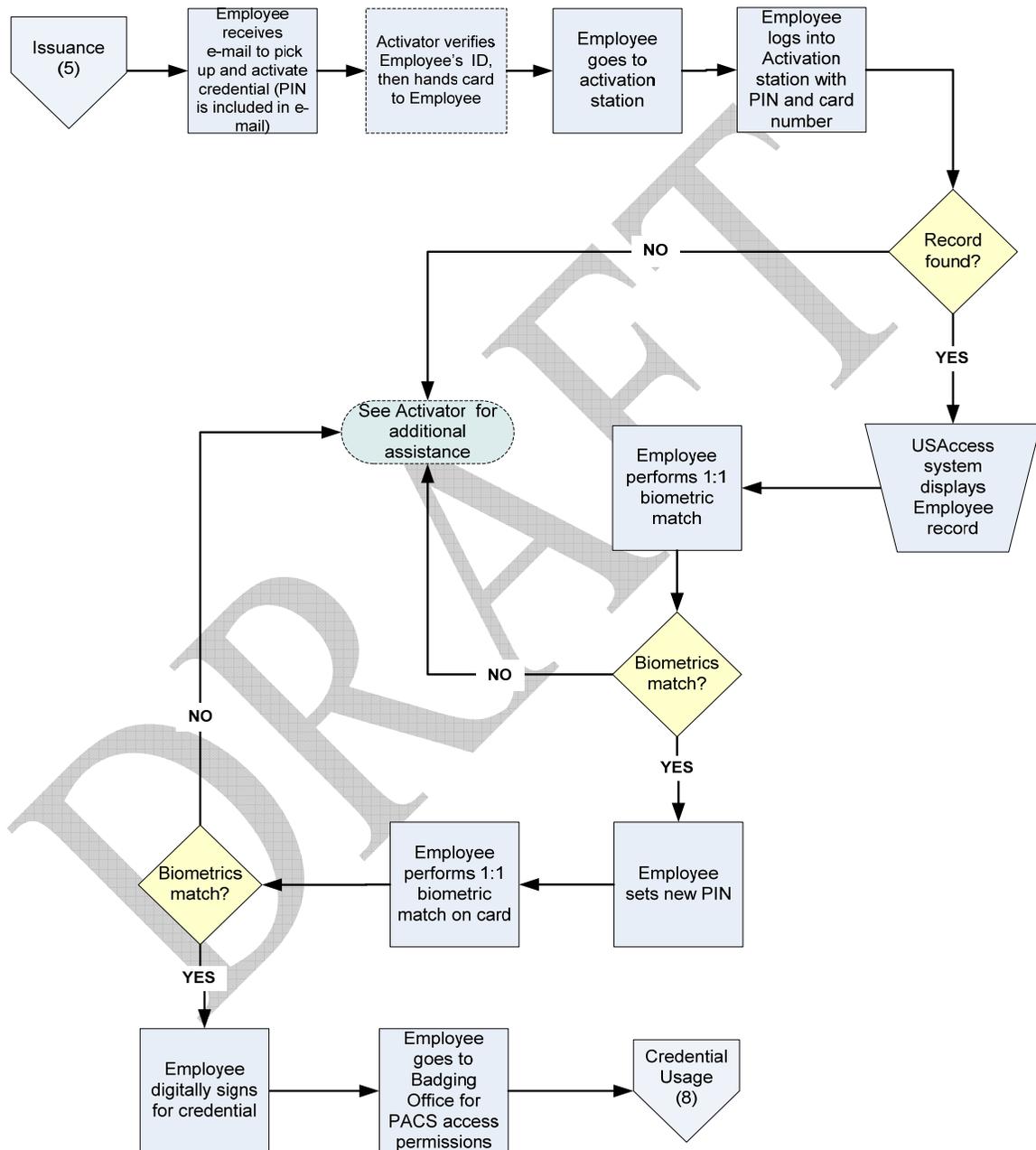
#### 11.1.1 Unattended Activation with Fingerprint Biometrics

This use case is based on a self-service model where the applicant is able to securely activate his or her own card. This scenario is only allowed when fingerprint biometrics are available. The Printing Facility ships the card to the designated shipping address specified by Sponsor, which will have an unattended activation station. The USAccess System will email the applicant a temporary system generated PIN. The applicant will use the Card Number and system generated PIN to authenticate to the activation portal. After a successful authentication of the applicant's fingerprint biometrics, it will be verified against the IDMS to validate the applicant, a new PIN will be set, the minutiae on the card will be verified, load the certificates, and have the applicant will digitally sign for the card.

When card activation fails, the Activator/Issuer will take back the card, flag that the card activation failed, note the reason why it failed, and abort the activation process. The card shall be submitted to the security officer for revocation & destruction. The Security Officer will mark in the System that the card was destroyed and submit a reprint request if warranted.

### 11.1.2 Detailed Unattended Activation Process

The following diagram details the workflow and steps described in this section cover the following use cases: (a) Unattended Activation with Fingerprint Biometrics and (b) Unattended Failed Activation.



6-1

Figure 47: Unattended Activation (6-1)

1. The Applicant receives an e-mail stating that their credential is ready to be activated.
2. The Activator/Issuer verifies that applicant information and card display information are correct. Activator/Issuer provides the Applicant with his/her inactivated LincPass.
3. The application then goes to the unattended activation station with their inactivated LincPass to complete activation process.
4. The applicant uses the card number (on the back of the card) and system generated PIN (provided to applicant from an e-mail) to log on to the activation web application.
5. Applicant information is displayed on the screen. If the person is not known to the USAccess System they need to see the enrollment station personnel.
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 card being unlocked.
7. The applicant sets his/her new PIN that is 6 to 8 digits in length.
8. The USAccess System tests the newly activated LincPass card by prompting the applicant to enter his/her PIN and biometric prints.
9. The USAccess System encodes the card with the digital certificates and will display "Successfully Encoded smart Card" status when finished.
10. The USAccess System will display "Card Successfully Activated."
11. The Applicant signs for the credential. (The Endorsement screen appears requiring the Applicant's acknowledgement of agreement to terms and conditions for receipt of the PIV Card?)
12. USAccess System will prompt the Applicant to remove the LincPass from the Smart Card Reader.
13. Applicant goes to the Badging Office for PACS access permissions.

## **11.2 Failed Unattended Activation**

If the applicant is unable to complete the unattended activation, the event will be logged in the System and the applicant will be directed to see an Activator/Issuer. (See attended activation or attended failed activation.)

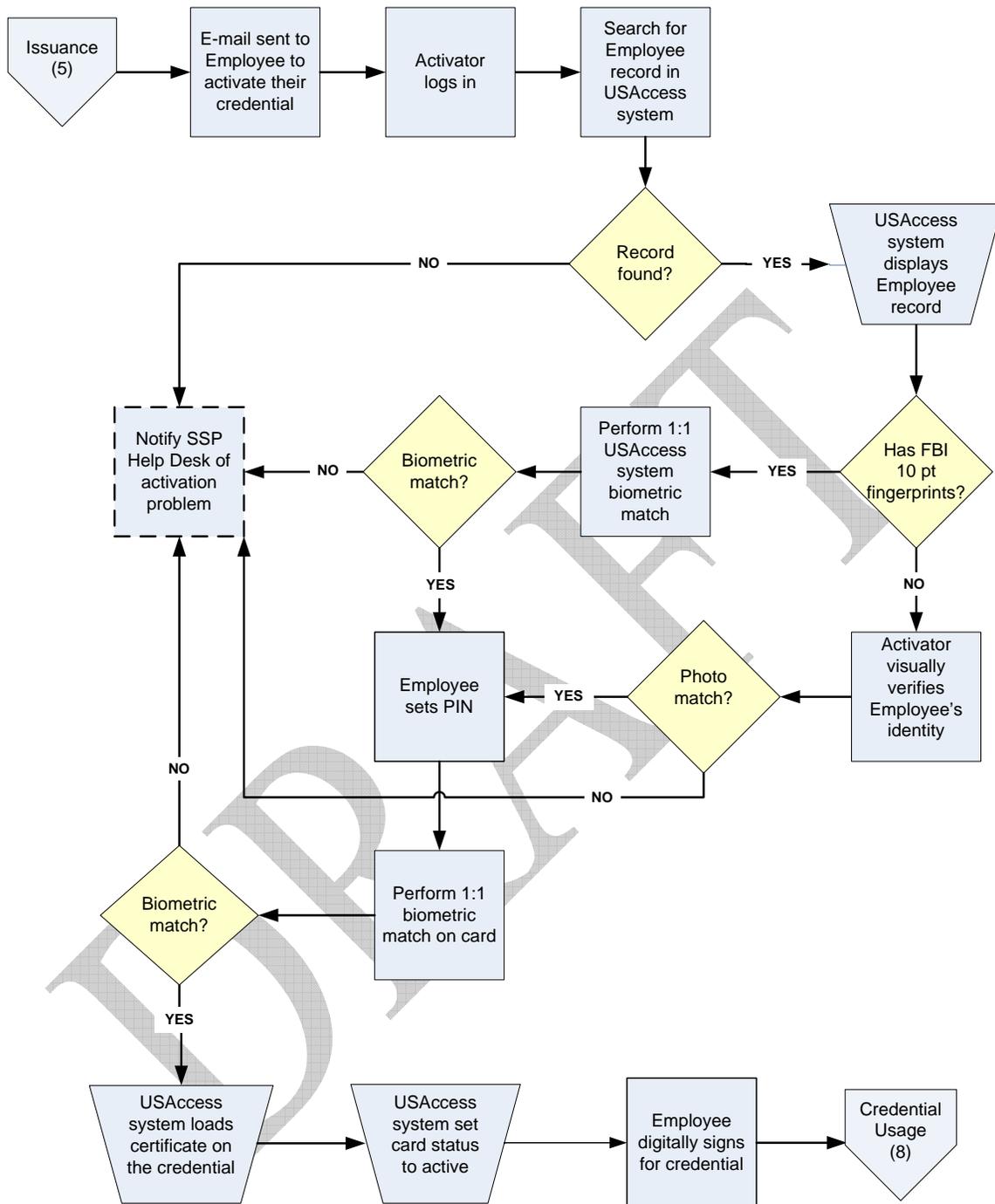
## **11.3 Attended Activation with Fingerprint Biometrics**

The Activation process starts when the applicant receives the card and goes through the steps of authenticating, finalizing and activating the card. For the initial deployment, the PIV card is distributed to a designated Activator/Issuer for an Agency. The Activator/Issuer takes the applicant through the card Activation process. First, the applicant is verified and biometrically authenticated, using biometric scans. Second, the system finalizes the personalization of the card by loading the required certificates and initialization of the PIN number. Third, the system updates and maintains the status of the PIV card and cardholder. The System shall use the applicant's fingerprint biometrics will be verified against the IDMS to validate the applicant, set the PIN, verify the minutiae on the card, load the certificates, and have the applicant digitally sign for the card.

## **11.4 Attended Activation Workflows**

### **11.4.1 Detailed Attended Activation Process EmpowHR**

USDA has planned to have mostly Unattended Activations throughout the Department. Applicants whose fingerprints cannot be captured must go to an Attended Activation Station. The following diagram details the workflow and steps described in this section cover the following use cases in EmpowHR: (a) Attended Activation with Fingerprint Biometrics, (b) Attended Activation without Fingerprint Biometrics and (c) Attended Failed.



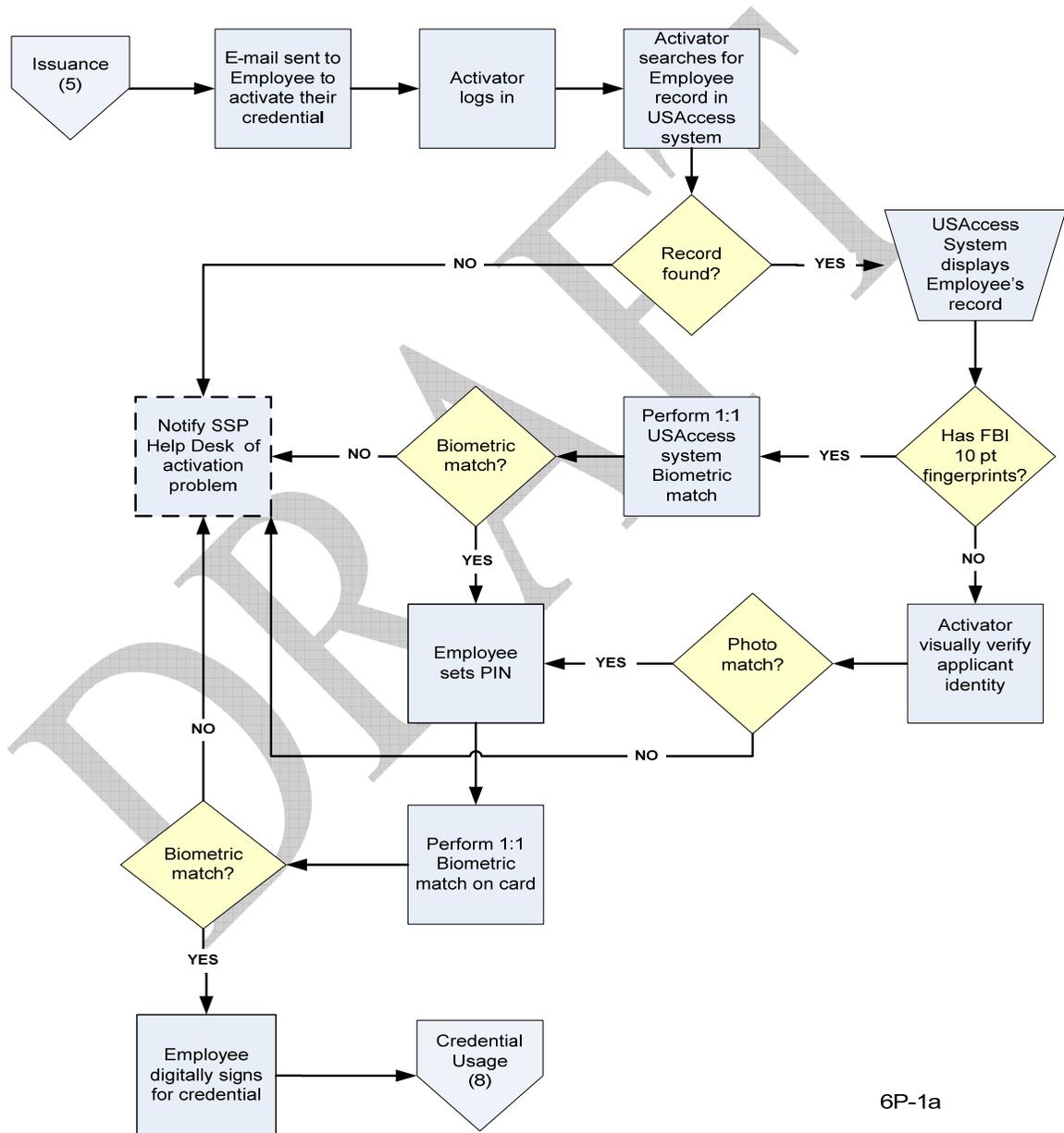
6E-1a

Figure 48: Attended Activation (6E-1a)

1. Activator/Issuer uses ID and password to logon to the activation USAccess web application.
2. The Activator/Issuer verifies that the applicant information and card display information are correct. The Activator/Issuer enters the unique card number into the system to search for the IDMS record.
3. If the IDMS record is not found, end the activation process and notify the SSP that no applicant record was found for the LincPass by setting the activation issue flag and noting the problem.
4. If the record is found, display applicant information on the screen. If there is no fingerprint record, the Activator/Issuer visually checks applicant facial image against the IDMS photo and the LincPass photo to verify that applicant information and card display info match.
5. If there are fingerprint records, the applicant provides the primary finger print using the biometric card reader for a 1:1 match in the IDMS database. A successful match will result in the card being unlocked.
6. If the photo does not match against the photo stores in the IDMS and/or the card Activator/Issuer will notify the SSP flag and note problem and ends activation session.
7. If photos match and biometric matched the applicant sets his/her PIN which must be 6-8 digits in length.
8. The applicant provides primary and secondary fingerprints so that the activation process can perform a 1:1 match of the biometric against the minutiae on the LincPass to ensure proper operation against the card.
9. If biometric does not match, the Activator/Issuer will notify the SSP flag and note problem and ends activation session.
10. After a new PIN is successfully, created the certificates (authentication, digital signature, and encryption keys) are loaded on the system.
11. The system tests the newly activated LincPass card by prompting the applicant to enter his/her PIN and biometric prints.
  - a. If test fails, notify SSP of activation problem.
  - b. If test is successful, system will display "Card Successfully Activated."
12. The applicant accepts the card by reading the acceptance notice and digitally signs for the card.

### 11.4.2 Detailed Attended Activation Process Payroll Personnel

The following diagram details the workflow and steps described in this section cover the following use cases in Payroll Personal: (a) Attended Activation with Fingerprint Biometrics, (b) Attended Activation without Fingerprint Biometrics and (c) Attended Failed.



6P-1a

Figure 49: Detailed Attended Activation in Payroll Personnel (6P-1a)

1. Activation Activator/Issuer uses ID and password to logon to the activation web application.
2. The Activator/Issuer verifies that the applicant information and card display information are correct. The Activator/Issuer enters the unique card number into the system to search for the IDMS record.
3. If the IDMS record is not found, end the activation process and notify the SSP that no applicant record was found for the LincPass by setting the activation issue flag and noting the problem.
4. If the record is found, display applicant information on the screen. If there is no fingerprint record, the Activator/Issuer visually checks applicant facial image against the IDMS photo and the LincPass photo to verify that applicant information and card display info match.
5. If there are fingerprint records, the applicant provides the primary finger print using the biometric card reader for a 1:1 match in the IDMS database. A successful match will result in the card being unlocked.
6. If the photo does not match against the photo stores in the IDMS and/or the card Activator/Issuer will notify the SSP flag and note problem and ends activation session.
7. If photos match and biometric matched the applicant sets his/her PIN which is 6-8 digits in length.
8. The applicant provides primary and secondary fingerprints so that the activation process can perform a 1:1 match of the biometric against the minutiae on the LincPass to ensure proper operation against the card.
9. If biometric does not match, the Activator/Issuer will notify the SSP flag and note problem and ends activation session.
10. After a new PIN is successfully, created, the certificates (authentication, digital signature, and encryption keys) are loaded on the system.
11. The system tests the newly activated LincPass card by prompting the applicant to enter his/her PIN and biometric prints.
  - a. If test fails, notify SSP of activation problem.
  - b. If test is successful, system will display "Card Successfully Activated."
12. The applicant accepts the card by reading the acceptance notice and digitally signs for the card.

### **11.5 Failed Attended Activation**

When card activation fails, the Activator/Issuer takes back the card, flags that the card activation failed, notes the reason why it failed, and aborts the activation process. The card is submitted to the Security Officer for revocation and destruction. The Security Officer marks in the system that the card was destroyed and submit a reprint request if warranted.

DRAFT

## Section 12 Security Officer

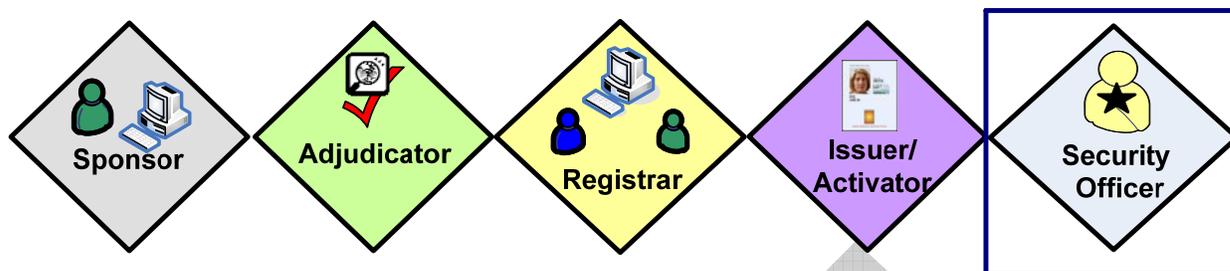


Figure 50: Security Officer Overview

The Security Officer is the individual authorized to physically collect revoked cards, and the daily contact for agency employees who lose their LincPasses.

There are three levels of security officers: USDA Department Security Officers, Agency Security Officers and Security Officers (includes personnel, IT, or physical security officers). USDA Department Security Officer can access all records. Agency Security Officers can only access records only for their designated agency, this officer must be a physical security job category.

The Security Officer is the individual authorized to physically collect revoked cards, and is the daily contact for agency employees who report missing, lost, or stolen PIV cards. It is also the only role in the USAccess System that has the ability to un-suspend a PIV credential.

A personnel security officer should be designated by each agency participating in USAccess. This person is responsible for the suspension and/or revocation of LincPasses and/or PIV certificates that result from personnel-related reasons. These reasons may include temporary suspension from work-related duties, maternity/paternity leave, leave of absence, resignation, and retirement, among other personnel situations. A personnel security officer should also vet any potential identity impersonation events.

A physical Security Officer should be designated by each agency participating in USAccess. This individual is responsible for the physical security of an agency's sites and/or facilities, including the physical access control systems (PACS).

A Security Officer has multiple duties within the system. They can include:

- Suspend a card for security related threats
- Collect and destroy card from cardholder whose sponsorship or status is terminated
- Reactivate a card
- Mark that a card was destroyed and document the reason.
- Re-issue a new card for existing card-holder
- Log a security event

- Investigate incidents with the Agency SO to resolve any discrepancies.
- Provide audit logs to designated government representatives on-demand
- Resolve issues/invalidate enrollments involving fraudulent source documents or variables
- Allow enrollment of previously enrolled applicant if deemed necessary
- Approve/Disapprove activation continuance
- Determine specifics of file modification event
- Approve/Disapprove rollback

Agency Security Officers shall be responsible for managing employees, contractors and affiliates “credential status change”, when required to immediately change the status of a card between active, suspended and revoked. Changes to the card status should occur within 30 minutes upon notification of a needed change.

1. OSS - GS-0080 job series - Physical Security Specialist at the Departmental Administration Level that will provide oversight for all Agency Security Officers.
2. Agency with GS-0080 job series - Most large agencies have Security Specialist within their organizations to provide for brick and mortar type security. Other agencies have something similar to a 0080 security specialist such as Law Enforcement Officers for the Forest Service and Homeland Security Officials for other agencies.
3. Agency without 0080 or like personnel, OSS will support those agencies as they do with their other physical security needs.

## 12.1 Security Officer Security Event Processes

The following diagram details the workflow of the processes performed by the Security Officer during security events.

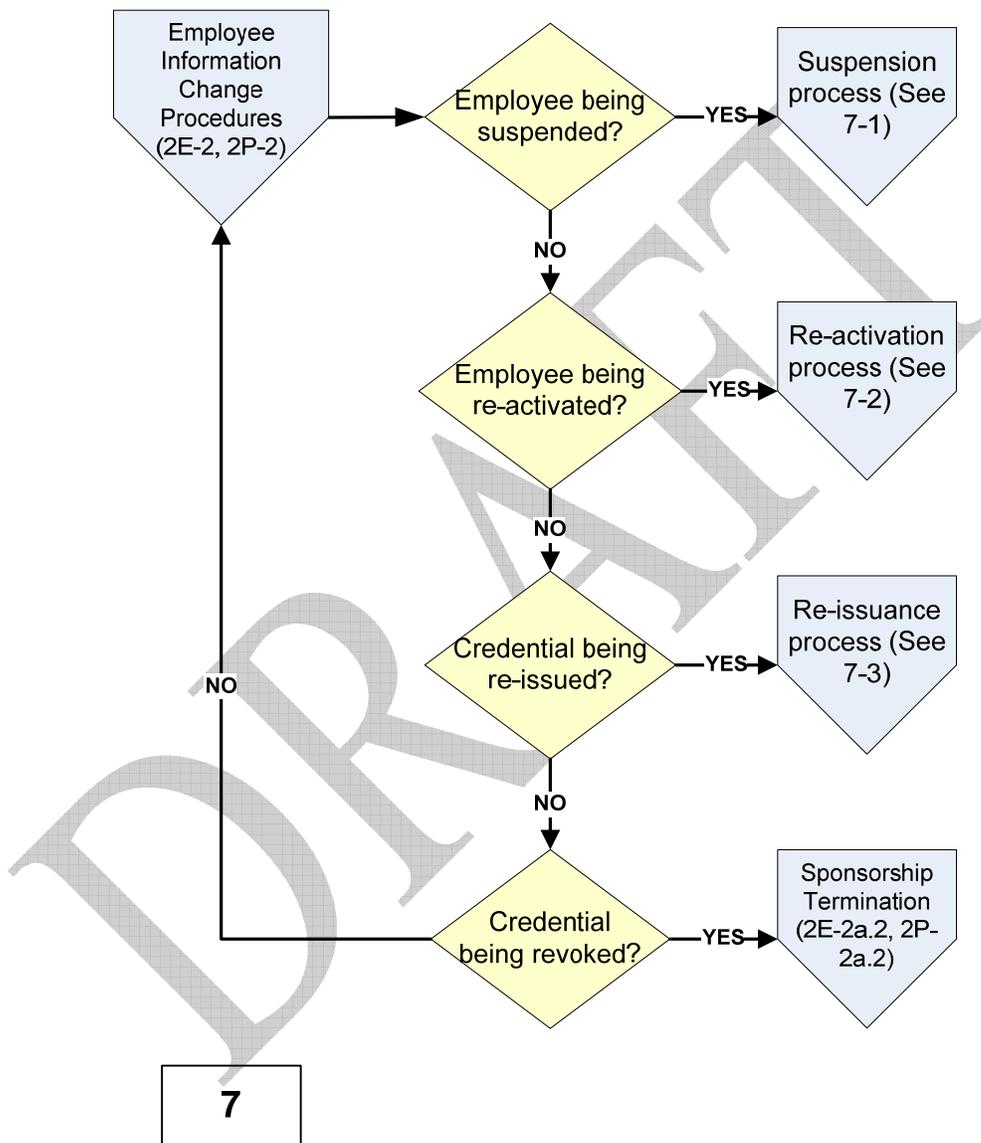


Figure 51: Security Officer Process (7)

1. If the Employee is being suspended, see the Suspension process (7-1).
2. If the Employee is being re-activated (from Suspension), see the Re-activation process (7-2).
3. If the Employee card is being re-issued, see the Re-Issuance process (7-3).

## 12.2 Security Officer Suspension Process

The following diagram details the workflow of the card suspension process performed by the Security Officer during security events.

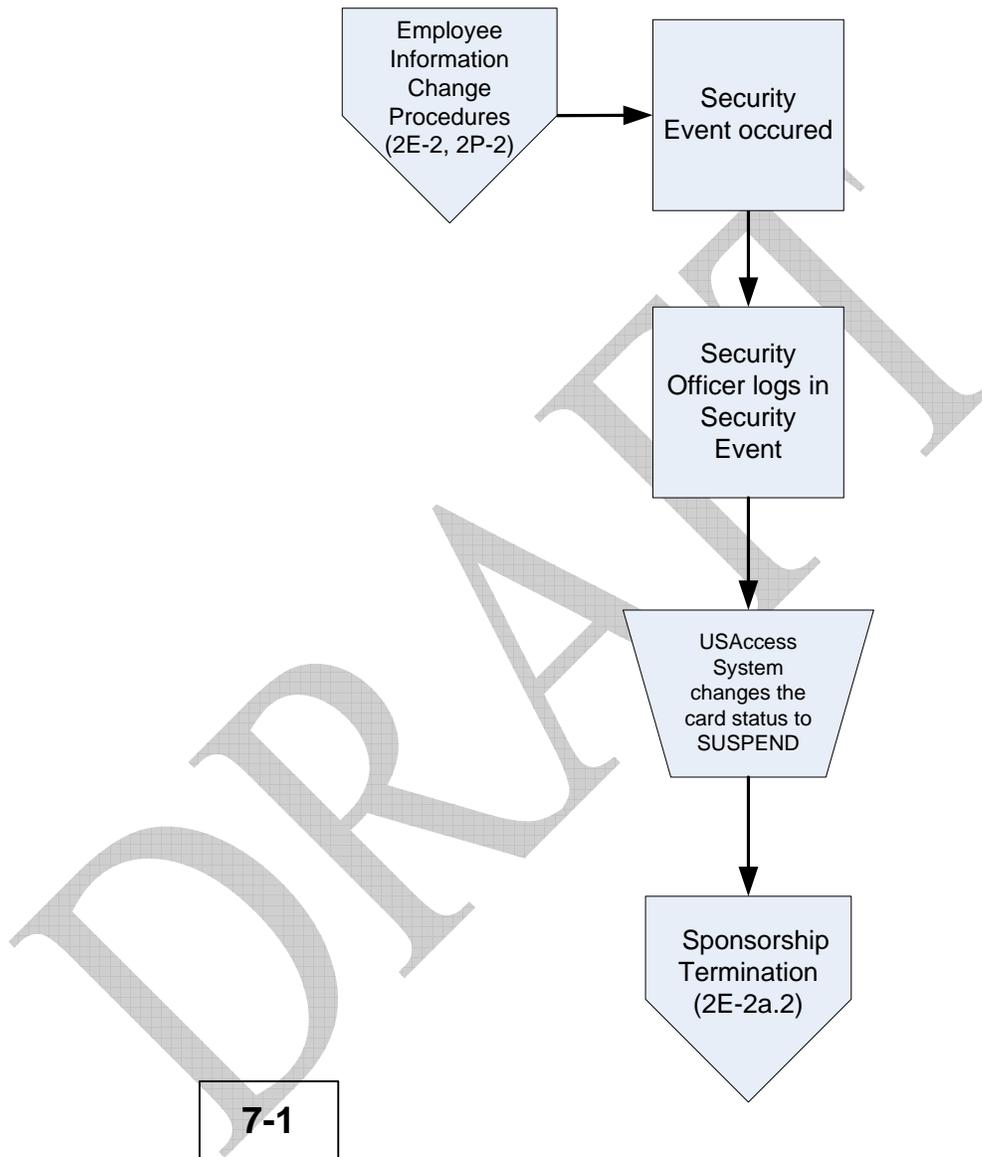


Figure 52: Security Officer Suspension (7-1)

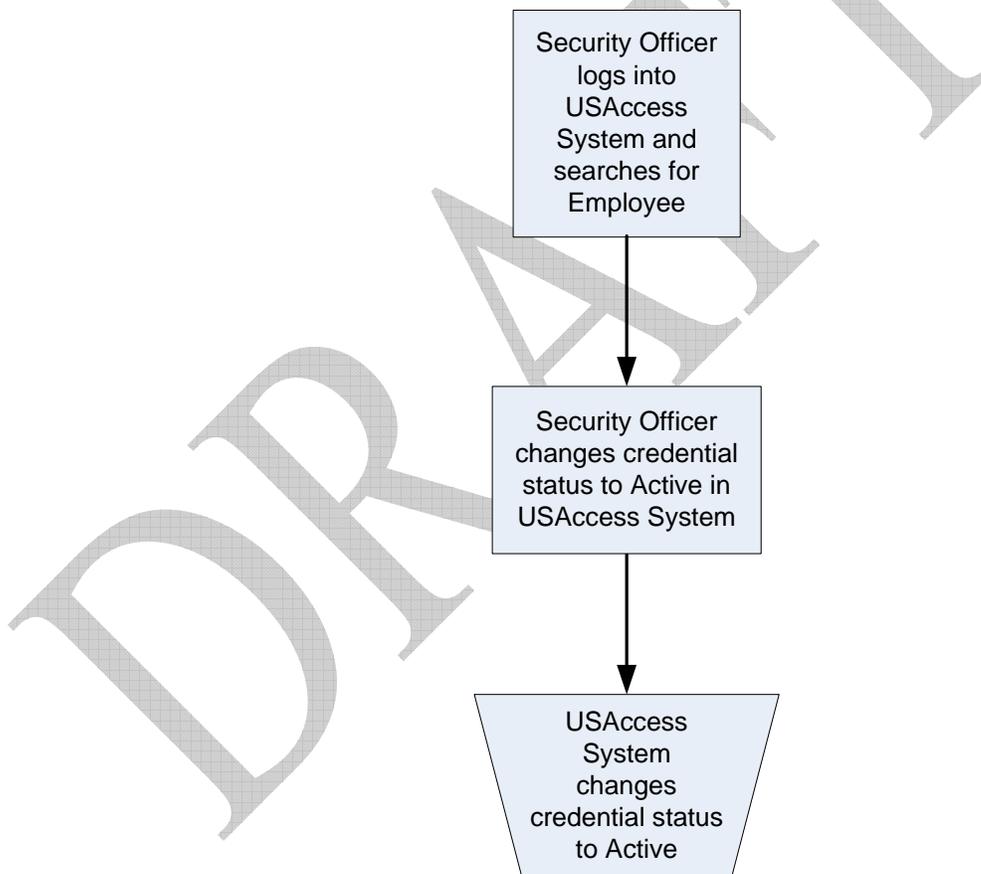
1. A security event occurs that requires investigation by the Security Officer.
2. The Security Officer logs into the USAccess System to record the security event sets the employment status to suspend, and saves the record. Saving this

change in the USAccess System will trigger an automatic suspension of the PIV card.

3. The USAccess System changes the card status to "SUSPEND".
4. The USAccess System suspends the certificates.

### 12.3 Security Officer Reactivation Process

The Reactivation process in this section is independent from any Employment Status changes in the authoritative HR systems (i.e. EmpowHR or Payroll Personnel) and applies only to manually changing the card status within the USAccess System. The following diagram details the workflow of the card reactivation process performed by the Security Officer during security events.



7-2

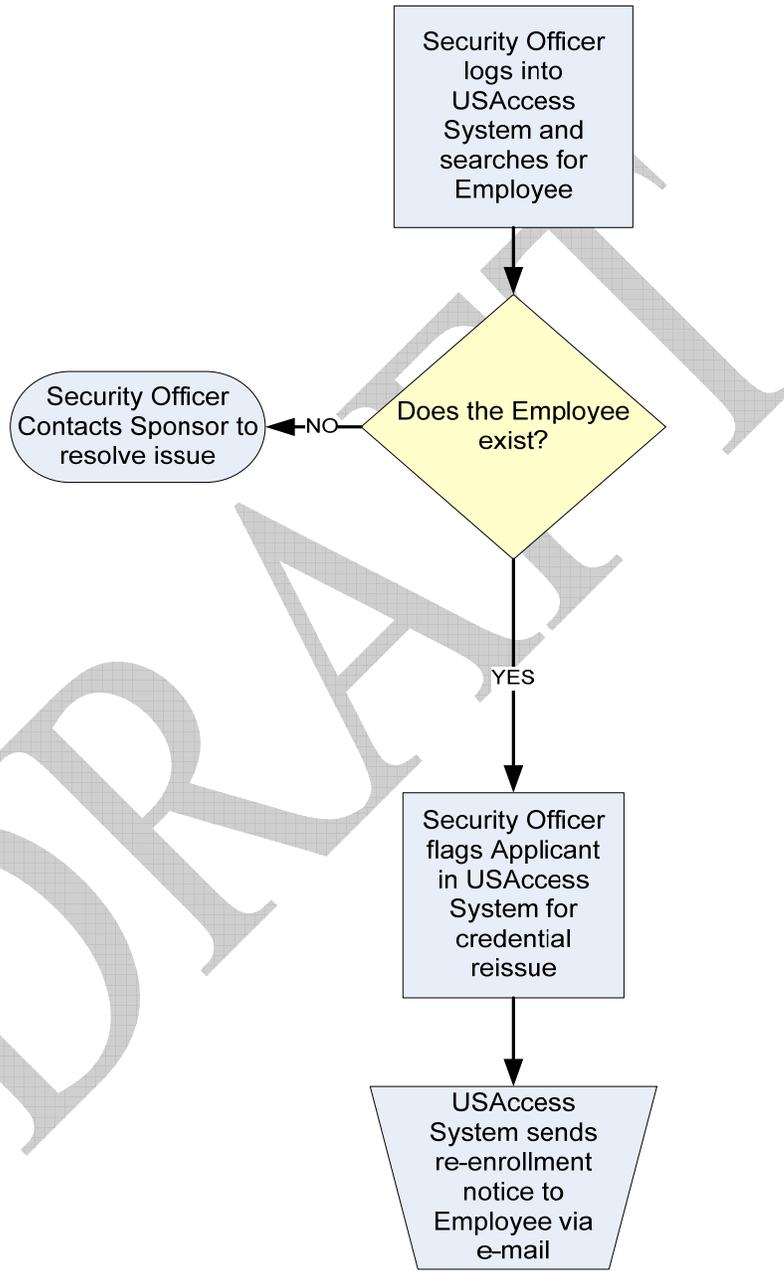
Figure 53: Security Officer Reactivation (7-2)

1. The Security Officer logs into the USAccess System and changes the card status to "ACTIVE".
2. The USAccess System submits reactivation certificates.
3. The systems are updated to reflect the suspension of the certificates.

DRAFT

### 12.4 Reissuance Process

The following diagram details the workflow of the card re-issuance process performed by the Security Officer during security events.



**7-3**

**Figure 54:** Security Officer Re-issuance in Payroll Personnel (7-3)

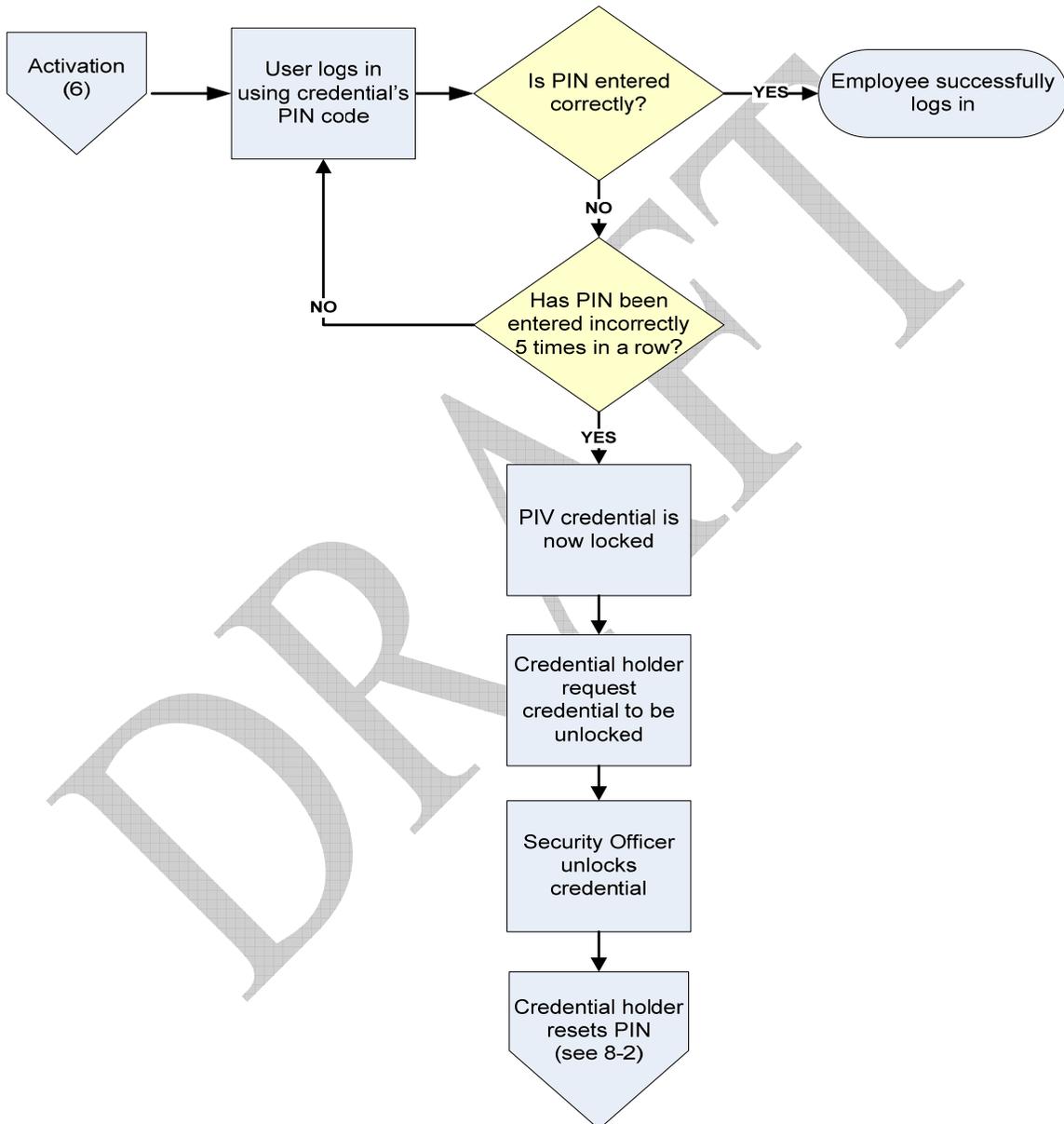
1. Security Officer logs into the USAccess System and searches for the applicant to determine if they are a new or existing applicant.
2. If the Applicant does not exist in the USAccess System, the Security Officer contacts the Sponsor
3. If the applicant exists in the USAccess System, their record is displayed in the sponsorship screen.
4. The Security Officer flags the Applicant for a card reissue, which will require the applicant to re-enroll and a new card to be issued.
5. The USAccess System makes the applicant eligible for enrollment.
6. The USAccess System automatically notifies the applicant of the re-enrollment via email. The email contains the sponsorship information so that the applicant can verify the accuracy of the data, and provides enrollment instructions.

DRAFT

## Section 13 Card Usage

### 13.1 PIN Unlock

The system provides capability to unlock the card once it has become locked due to 5 unsuccessful attempts by the Cardholder to enter the PIN.



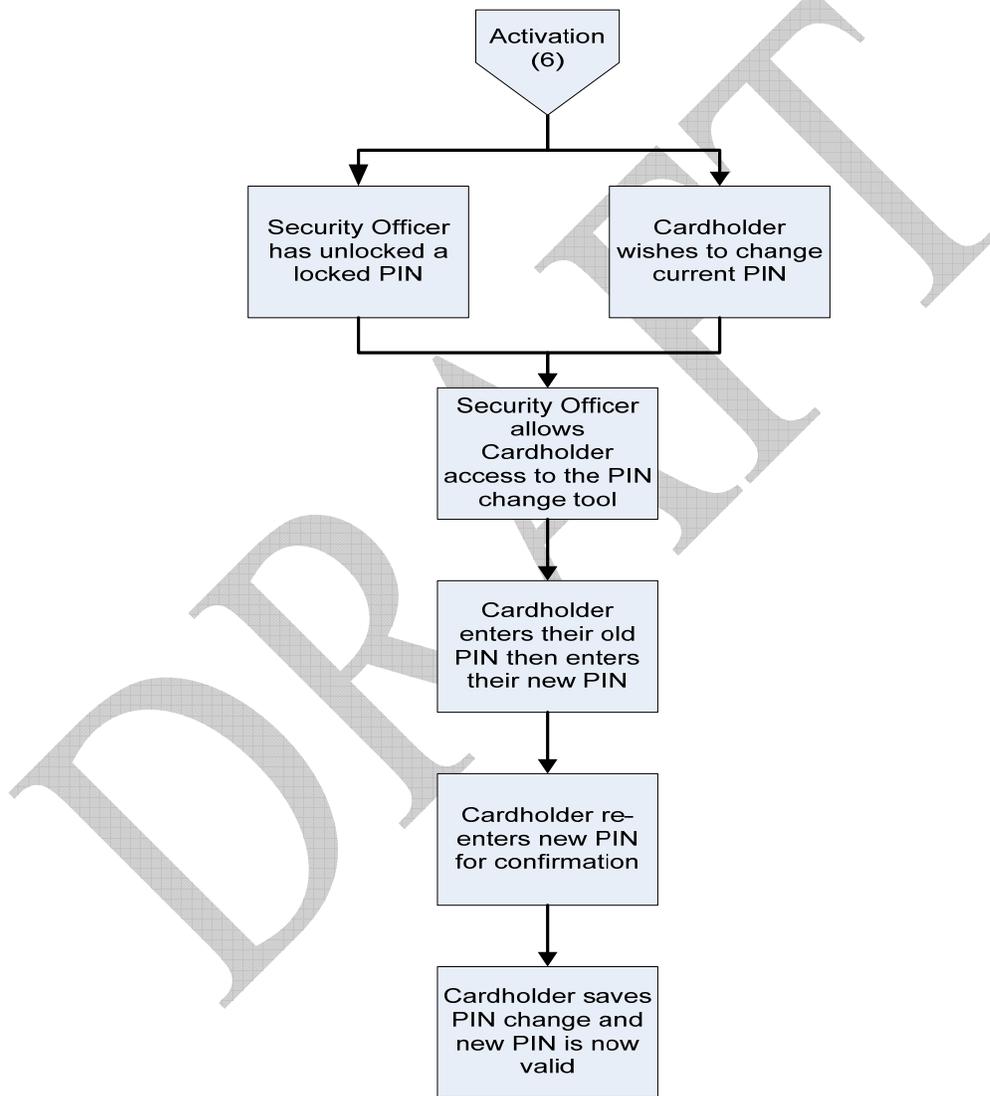
8-1

Figure 55: Card Usage-Pin Unlock (8-1)

1. The Cardholder enters the incorrect PIN 5 times in a row and locks out their card.
2. The Cardholder goes to the Security Officer to request the PIN be unlocked.
3. The Security Officer unlocks the PIN in the USAccess System.
4. The Cardholder must now reset their PIN.

### 13.2 PIN Reset

The PIN reset function provides the ability for the cardholder to change the existing PIN number to a new PIN number at any time during the card lifecycle.



8-2

Figure 56: Card Usage-Pin Reset (8-2)

1. The Cardholder needs to reset their PIN because it was previously locked or because they want a new PIN.
2. The Security Officer gives the Cardholder access to the PIN change tool in the USAccess System.
3. The Cardholder enters their old PIN along with a new PIN.
4. The Cardholder re-enters the new PIN for confirmation.
5. The Employee saves the new PIN and the PIN is now valid.

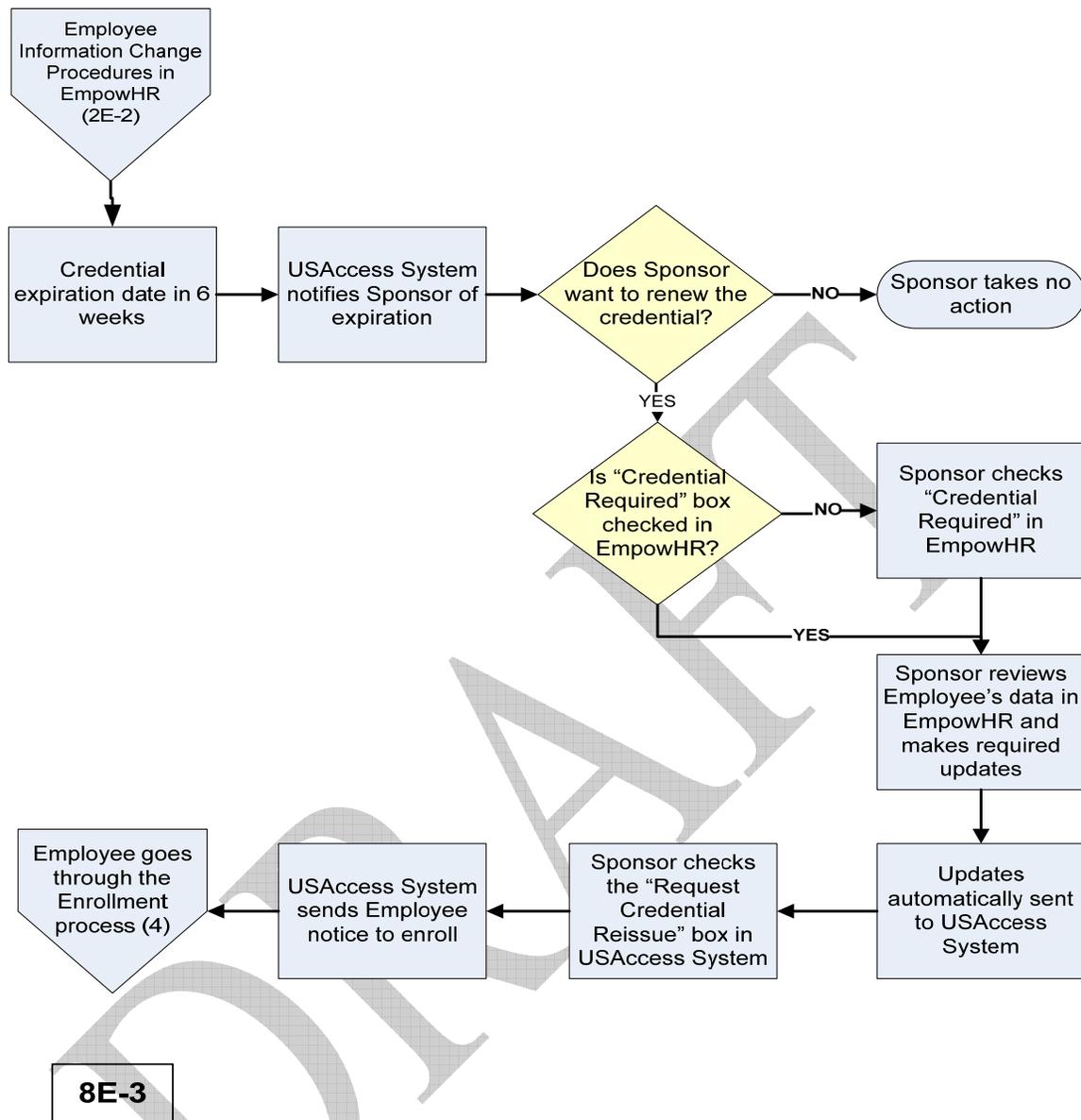
### **13.3 Card Renewal**

Renewal is the process by which a PIV Card is replaced after 5 years of use. The card renewal process is the same as the Card Reissue process, except that the Sponsor will be notified automatically 6 weeks prior to expiration of the card.

#### **13.3.1 EmpowHR Card Renewal Process**

The following diagram details the workflow of the card renewal process in EmpowHR.

DRAFT



**8E-3**

Figure 57: EmpowHR Card Renewal Process (8E-3)

1. The Sponsor receives an automated notice from the USAccess System 6 weeks prior to the expiration of the Employee's card; cards expire 5 years after initial issuance.
2. Does the Sponsor want to renew the card? If no, the Sponsor takes no action. If yes, the Sponsor checks to see if the "Card Required" box is checked in EmpowHR.
3. If the box is not checked, the Sponsor checks the box then reviews the Employee's information and makes any necessary updates.
4. The USAccess System is automatically updated from EmpowHR with any changes.
5. The Sponsor logs into the USAccess System and checks the "Request Card Re-Issue" box.



6. The USAccess System makes the Employee eligible for enrollment.
7. The USAccess System sends the Employee notification that they can enroll for their renewed card.
8. The Employee utilizes the Enrollment process (see Section 9) to get their card.

DRAFT

### 13.3.2 Payroll Personnel Card Renewal Process

The following diagram details the workflow of the card renewal process in Payroll Personnel

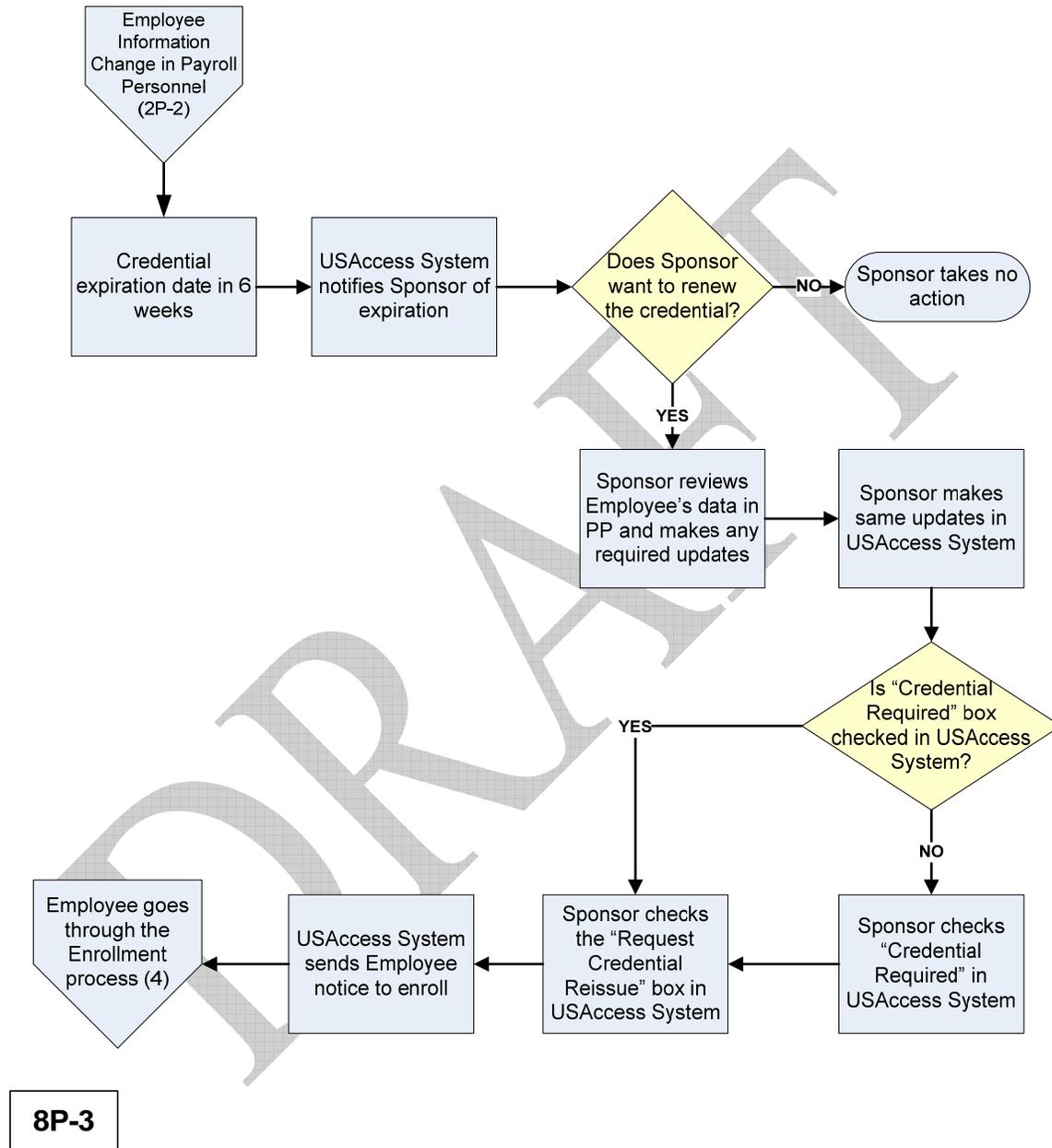


Figure 58: Card Renewal in Payroll Personnel (8P-3)

1. The Sponsor receives an automated notice from the USAccess System 6 weeks prior to the expiration of the Employee's card; cards expire 5 years after initial issuance.



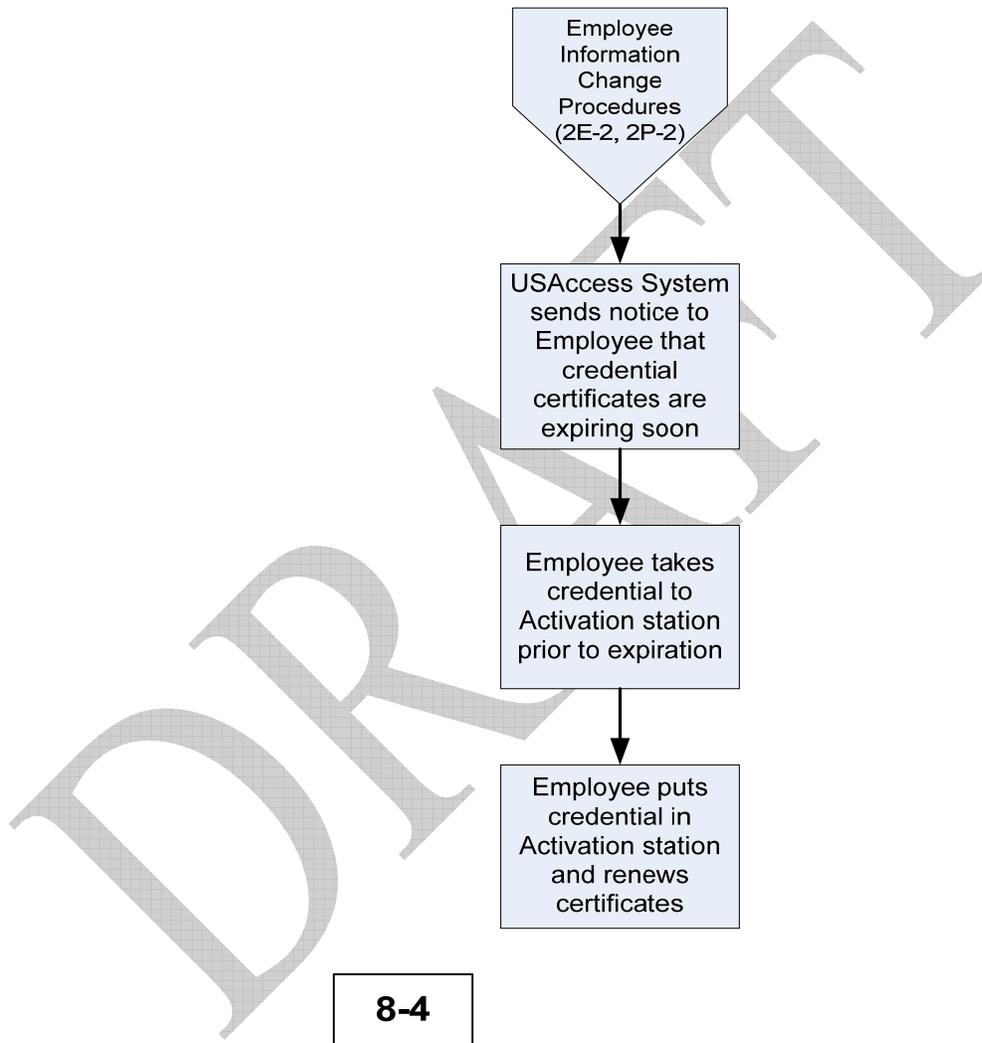
2. Does the Sponsor want to renew the card? If no, the Sponsor takes no action. If yes, the Sponsor reviews the Employee's information in Payroll Personnel and makes any necessary updates.
3. The Sponsor logs into the USAccess System and makes the same information updates.
4. If the "Card Required" box is not checked, the Sponsor checks the box.
5. The Sponsor checks the "Request Card Re-Issue" box.
6. The USAccess System makes the Employee eligible for enrollment.
7. The USAccess System sends the Employee notification that they can enroll for their renewed card.
8. The Employee utilizes the Enrollment process (see Section 9) to get their card

DRAFT

## 13.4 Attended Certificate Renewal

### Attended Certificate Renewal Process

This is the process by which a cardholder brings their card to an activation station to have the certificate (which has a 3 year expiration vs. the 5 year expiration for the card) renewed.



**Figure 59:** Attended Certificate Renewal (8-4)

1. The USAccess System sends the Employee a notice that their certificates are due to expire soon; certificates expire 3 years after being issued.
2. The Employee goes to the Activation station with their card.
3. The Employee renews the certificates on the card via the Activation station.
4. No new card is required during a certificate renewal

### 13.5 Unattended Certificate Renewal

#### Unattended Certificate Renewal Process

This is the process by which a cardholder renews the certificates (which has a 3-year expiration vs. the 5-year expiration for the card) in a self-service manner.

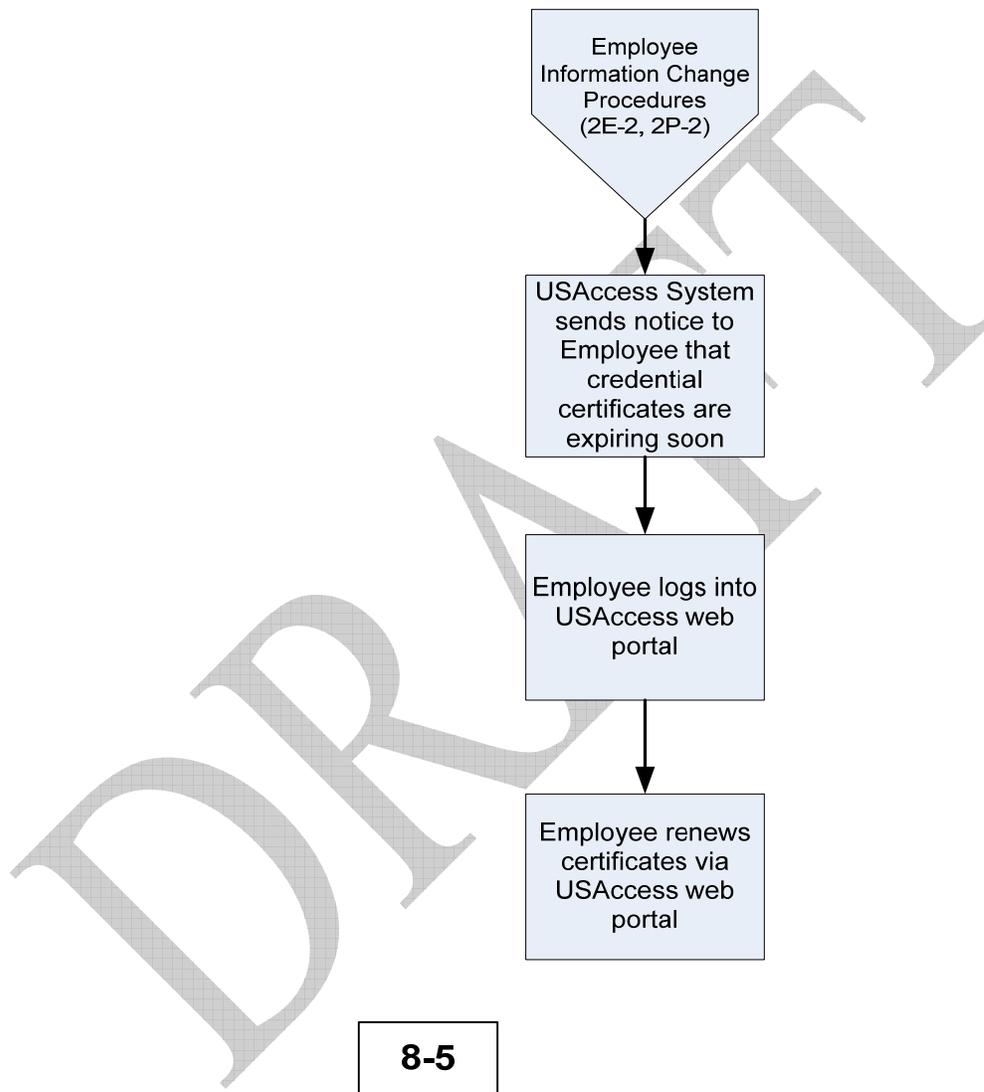


Figure 60: Unattended Certificate Renewal (8-5)

1. The USAccess System sends the Employee a notice that their certificates are due to expire soon; certificates expire 3 years after being issued.
2. The Employee logs into the USACCESS Web Portal
3. The Employee renews the certificates on the card via the web portal.
4. No new card is required during a certificate renewal



## Appendix A Acronyms

Acronym	Definition
ACL	Access Control List
BI	Background Investigation
CA	Certification Authority
CHUID	Cardholder Unique Identifier
DM	Departmental Manual
DR	Departmental Regulation
e-QIP	Electronic Questionnaires for Investigations Processing
FBI	Federal Bureau of Investigation
FBI Fingerprint Check	FBI National Criminal History Fingerprint Check
FIPS 201-1	Federal Information Processing Standard Publication 201-1
GSA	General Services Administration
HR	Human Resources
HRSD	Human Resources Service Division
HSPD-12	Homeland Security Presidential Directive 12
IDMS	Identity Management System
LACS	Logical Access Control System
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NCR	National Capital Region
NIST	National Institute for Standards and Technology
OCIO	Office of the Chief Information Office
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPM/NS BI	Office of Personnel Management or National Security Community Background Investigation
OPPM	Office of Procurement and Property Management
OSS	Office of Security Services
PACS	Physical Access Control System
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification, Part I
PIV-II	PIV-II Personal Identity Verification, Part II
PDSD	Personnel and Document Security Division



Acronym	Definition
PKI	Public Key Infrastructure
POC	Point of Contact
SF	Standard Form
SOI	Security Office Identifier
SON	Submitting Office Number
SP	Special Publication
SSP	Shared Services Process
USDA	United States Department of Agriculture

DRAFT



## Appendix B Sponsorship and Adjudication Forms

### LISTS OF ACCEPTABLE DOCUMENTS

LIST A		LIST B		LIST C
Documents that Establish Both Identity and Employment Eligibility	<b>OR</b>	Documents that Establish Identity	<b>AND</b>	Documents that Establish Employment Eligibility
1. U.S. Passport (unexpired or expired)		1. Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address		1. U.S. social security card issued by the Social Security Administration (other than a card stating it is not valid for employment)
2. Certificate of U.S. Citizenship (INS Form N-560 or N-561)		2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address		2. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350)
3. Certificate of Naturalization (INS Form N-550 or N-570)		3. School ID card with a photograph		3. Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal
4. Unexpired foreign passport, with I-551 stamp or attached INS Form I-94 indicating unexpired employment authorization		4. Voter's registration card		4. Native American tribal document
5. Permanent Resident Card or Alien Registration Receipt Card with photograph (INS Form I-151 or I-551)		5. U.S. Military card or draft record		5. U.S. Citizen ID Card (INS Form I-197)
6. Unexpired Temporary Resident Card (INS Form I-688)		6. Military dependent's ID card		6. ID Card for use of Resident Citizen in the United States (INS Form I-179)
7. Unexpired Employment Authorization Card (INS Form I-688A)		7. U.S. Coast Guard Merchant Mariner Card		7. Unexpired employment authorization document issued by the INS (other than those listed under List A)
8. Unexpired Reentry Permit (INS Form I-327)		8. Native American tribal document		
9. Unexpired Refugee Travel Document (INS Form I-571)		9. Driver's license issued by a Canadian government authority		
10. Unexpired Employment Authorization Document issued by the INS which contains a photograph (INS Form I-688B)		<b>For persons under age 18 who are unable to present a document listed above:</b>		
		10. School record or report card		
		11. Clinic, doctor or hospital record		
		12. Day-care or nursery school record		

Illustrations of many of these documents appear in Part 8 of the Handbook for Employers (M-274)



Personal Identity Verification II (PIV-II)  
Business Process, Sponsorship and Adjudication  
Policies and Procedures

Version 1.0



Office of Procurement and Property Management  
Personnel & Document Security Division

**Personnel Security Checklist**

NAME	SSN
AGENCY	POSITION

I. The following forms were submitted by your office and were found to be incomplete or improperly prepared. Please review the information below and resubmit the corrected forms **WITHIN 30 DAYS** or your case will be closed without action. All signatures and hand-written information must be in **BLACK INK**.

\_\_\_\_\_ **Cover Memo: The following information was not provided:**

- Provide:  Type of BI requesting  Accounting Code  Level of Clearance Required  
 Other \_\_\_\_\_

\_\_\_\_\_ **SF-86/ SF-85P/ SF-85**

- Sign  Date  Initial and redate Page 9 and 10  Update Item/s # \_\_\_\_\_  
 Complete Item/s # \_\_\_\_\_  
 Initial all write-overs, cross-outs, white-outs (Page/s \_\_\_\_\_)  
 Account for timeframe, from/to \_\_\_\_\_, Item # \_\_\_\_\_  
 Account for timeframe, from/to \_\_\_\_\_, Item # \_\_\_\_\_  
 Account for timeframe, from/to \_\_\_\_\_, Item # \_\_\_\_\_  
 Other \_\_\_\_\_

\_\_\_\_\_ **Resume, OF 612, or SF-171** (One of these items is required by OPM for first time, initial investigations.)

- Sign  Date  Complete Item/s # \_\_\_\_\_  Other: \_\_\_\_\_

\_\_\_\_\_ **OF-306** (Declaration Federal Employment)

- Sign  Date  Complete Item/s # \_\_\_\_\_  Other: \_\_\_\_\_

\_\_\_\_\_ **FD-258/SF-87** (Fingerprint Cards)

- Sign  Date  Complete Item/s # \_\_\_\_\_  Other: \_\_\_\_\_  
 Unclassifiable; submit new cards

\_\_\_\_\_ **Fair Credit Release Form**

- Sign  Date  Complete Item/s # \_\_\_\_\_  Other: \_\_\_\_\_

**II. PERSONNEL SECURITY DIVISION:**

Signature, PSD Security Specialist/Assistant: \_\_\_\_\_ Date: \_\_\_\_\_

**III. INITIATING OFFICE:**

The necessary corrective actions have been made on the forms indicated above. *The applicant has verified the corrective actions that were made.* The corrected forms and/or appropriate copies are attached.

Signature, Initiating Office Representative: \_\_\_\_\_ Date: \_\_\_\_\_

PSD WS1 (1/03)



United States  
Department of  
Agriculture

LETTER OF INQUIRY TEMPLATE

Privacy Act Material

Return Receipt Requested

[Date]

[Subject's name]

[Street address]

[City, State & Zip Code]

Dear [Subject],

Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, requires Applicants for the U.S. Department of Agriculture Personal Identity Verification (PIV) I.D. Badge to undergo a background investigation to determine their eligibility to hold that Badge. The U.S. Office of Personnel Management has completed your background investigation. That investigation developed issues which must be addressed prior to making an eligibility decision.

Please provide this office written responses to the question(s) below. Providing response(s) to the attached questions is voluntary. However, without this information, we may not be able to make a final decision on your application for a PIV I.D. Badge. This will affect your employment with [agency name]. **A false answer to any of the question(s) below may be grounds for denying or revoking your PIV I.D. Badge and terminating your employment.** The information you provide will be considered in reviewing your eligibility and will be protected from unauthorized disclosure under the Privacy Act of 1974.

Issue: [List issue, i.e., Criminal Convictions]

The Concern: [List eligibility concern, i.e., a history or pattern of criminal activity creates doubt about a person's judgment, reliability, and trustworthiness.]

According to the OPM Report of Investigation, you were convicted [list convictions and develop questions].



**USDA PIV I.D. BADGE ADJUDICATION WORKSHEET**

<i>SUITABILITY FACTORS (5 CFR 731.202 B), ADDITIONAL CONSIDERATIONS (5 CFR 731.202 C) &amp; DM-3800-001</i>	
<b>Misconduct or Negligence in Employment</b>	
<input type="checkbox"/> Incident(s) has no bearing on this position <input type="checkbox"/> Incident(s) was not recent <input type="checkbox"/> Incident occurred as a minor <input type="checkbox"/> Successful Rehabilitation	
Narrative: _____	
<b>Criminal or Dishonest Conduct</b>	
<input type="checkbox"/> Incident(s) has no bearing on this position <input type="checkbox"/> Incident(s) was not recent <input type="checkbox"/> Incident occurred as a minor <input type="checkbox"/> Successful Rehabilitation <input type="checkbox"/> Debts are not of a significant nature.	
Narrative: _____	
<b>Material Intentional False Statement or Deception or Fraud in Examination or Appointment</b>	
<input type="checkbox"/> Incident(s) has no bearing on this position <input type="checkbox"/> Incident(s) was isolated <input type="checkbox"/> Incident was not deliberate	
Narrative: _____	
<b>Refusal to Furnish Testimony as Required by Section 5.4 (Civil Service Rule)</b>	
Narrative: _____	
<b>Alcohol Abuse</b>	
<input type="checkbox"/> Incident(s) was isolated <input type="checkbox"/> Incident(s) was not recent <input type="checkbox"/> Incident occurred as a minor <input type="checkbox"/> Successful Rehabilitation <input type="checkbox"/> Not of a nature or duration that has prevented Subject from performing his/her duties	
Narrative: _____	
<b>Illegal Use of Narcotics Drugs or Other Controlled Substances</b>	
<input type="checkbox"/> Incident(s) was isolated <input type="checkbox"/> Incident(s) was not recent <input type="checkbox"/> Incident occurred as a minor <input type="checkbox"/> Successful Rehabilitation	
Narrative: _____	
<b>Knowing and Willful Engagement in Acts or Activities Designed to Overthrow the U.S. Government by Force</b>	
Narrative: _____	
<b>(1) Was Applicant's True Identity Confirmed, and (2) Any Statutory or Regulatory Bar which prevents the lawful employment of the person involved in the position in question.</b>	
Narrative: _____	



## Appendix C References

These are the major resources used to develop this document.

Title	Date
Personal Identity Verification (PIV) of Federal Employees and Contractors	March, 2006
User Interface Specification Document	February, 2007
GSA HSPD-12 Solicitation No. TQ-PLB-07-0002, RFQ #186901	February 8, 2007
Use Cases (Technical) Priority 1	March 13, 2007
PIV Policy, Version 1.0	June 2, 2007
USDA Adjudicators FAQ	March 28, 2006
OPPM PDSD ID Card Examination and Validation	OPPM PDSD ID Card Examination and Validation
Draft PIV ID Badge BI Requirements	March 24, 2006
Amended Applicant FAQ	March 28, 2006
USDA Sponsors FAQ	October 12, 2005
2 <sup>nd</sup> Amended Registrars FAQ	March 28, 2006
Amended USDA Adjudicators FAQ	March 28, 2006

DRAFT



## Appendix D Data Preparation

### USDA LincPass

HSPD-12 LincPass

### Data Preparation Checklist for Payroll/Personnel Agency

As of 12 July 2007

This document provides a quick iterative checklist for the USDA Human Resource (HR) staff to follow for verifying/updating employee records for the HSPD-12 LincPass.

Step	Instructions	Complete
<b>HR Instructions</b>		
1	Working with the Logistics Team, identify a Sponsor and Adjudicator for a given location or set of data.	
2	Identify records based on Enrollment Station Location	
3	Identify active employees within your agency (or supported agency) who should receive an HSPD-12 LincPass	
5	Identify Federal Employees from that location that have successfully completed an FBI or higher background investigation	
6	Verify accuracy of employee name information in the front-end system that feeds Payroll Personnel, ie. EPIC. Fix issues for all employees (ie. Suffix combined in last name field) in the front-end HR system	
7	Identify all non-US citizens and update those records in the front-end to Payroll Personnel system.	
<b>Employee Instructions</b>		
8	Update Business Email and Phone within eAuthentication by doing the following: 1. Browse to <a href="http://www.eauth.egov.usda.gov">http://www.eauth.egov.usda.gov</a> 2. Click on "Update Your Account". 3. Click "Continue" at the purple <i>Warning</i> screen. 4. Log in with your eAuthentication User ID and password. The "Welcome to IdentityMinder" screen will display. 5. If you have a Level 2 account, click on the "My Account" link. If you have a Level 1 account, proceed to step 6. 6. Click on "Modify my profile". 7. Make desired changes in the online form, and then click the "submit" button in the bottom right corner to save the information. 8. You may now click on "Logout" (in the upper right corner) to log out.	
<b>HR Instructions</b>		
9	Sponsor Login to secure web-site (URL to follow)	
10	Flag, certify and submit the prepared records (Instructions to follow)	
11	Data Prep Team will inform Sponsor of record submission to GSA and data readiness to use GSA portal	
12	Identify all Emergency Response Officials and update those records in the GSA web portal following GSA's instructions.	
13	Verify adjudication result has been entered into GSA web portal, if it hasn't, update those records following GSA's instructions.	
14	<b>Start Preparing the next set of records (return to Step 1)</b>	

Please email [hspd12@ftc.usda.gov](mailto:hspd12@ftc.usda.gov) or call the LincPass hotline at 202-720-9042 if you have questions.



**USDA LincPass**

**HSPD-12 LincPass  
Data Preparation Checklist for EmpowHR Agency**

As of 12 July 2007

This document provides a quick iterative checklist for the USDA Human Resource (HR) staff to follow for verifying/updating employee records for the HSPD-12 LincPass.

Step	Instructions	Complete
<b>HR Instructions</b>		
1	Working with the Logistics Team, identify a Sponsor and Adjudicator for a given location or set of data.	
2	Identify records based on Enrollment Station Location	
3	Identify active employees within your agency (or supported agency) who should receive an HSPD-12 LincPass	
4	Identify Federal Employees from that location that have successfully completed an FBI or higher background investigation	
5	Verify adjudication result has been entered into EmpowHR, if it hasn't, update those records following the HSPD-12 ProcedureToVerifyEmplRecordsInEmpowHR_v3.doc	
6	Verify accuracy of employee name information in EmpowHR. Fix issues for all employees (ie. Suffix combined in last name field) in the EmpowHR system following the HSPD-12 ProcedureToVerifyEmplRecordsInEmpowHR_v3.doc	
7	Identify all non-US citizens and update those records in the EmpowHR system following the HSPD-12 ProcedureToVerifyEmplRecordsInEmpowHR_v3.doc.	
8	Identify all Emergency Response Officials and update those records in the EmpowHR system following the HSPD-12 ProcedureToVerifyEmplRecordsInEmpowHR_v3.doc.	
<b>Employee Instructions</b>		
9	<p>Update Business Email and Phone as follows:</p> <p>If your Employees have been trained to use the EmpowHR self-service module, update this information by following the HSPD-12_ProcedureToVerifyEmplRecordsInEmpowHR_v3.doc.</p> <p>If not, update this information within eAuthentication by doing the following:</p> <ol style="list-style-type: none"> <li>1. Browse to <a href="http://www.eauth.egov.usda.gov">http://www.eauth.egov.usda.gov</a></li> <li>2. Click on "Update Your Account".</li> <li>3. Click "Continue" at the purple <i>Warning</i> screen.</li> <li>4. Log in with your eAuthentication User ID and password. The "Welcome to IdentityMinder" screen will display.</li> <li>5. If you have a Level 2 account, click on the "My Account" link. If you have a Level 1 account, proceed to step 6.</li> <li>6. Click on "Modify my profile".</li> <li>7. Make desired changes in the online form, and then click the "submit" button in the bottom right corner to save the information.</li> <li>8. You may now click on "Logout" (in the upper right corner) to log out.</li> </ol>	
<b>HR Instructions</b>		
10	Sponsor Login to secure web-site (URL to follow)	
11	Flag, certify and submit the prepared records (Instructions to follow)	
12	<b>Start Preparing the next set of records (return to Step 1)</b>	

Please email [hspd12@ftc.usda.gov](mailto:hspd12@ftc.usda.gov) or call the LincPass hotline at 202-720-9042 if you have questions.

USDA LincPass

HSPD-12 LincPass Rollout  
Procedures to Verify/Update Employee Records in EmpowHR

As of 31 July 2007

This document provides detailed procedures to USDA Human Resource (HR) staff for verifying/updating employee records in EmpowHR for the initial USDA LincPass rollout. Employee records must be verified and updated to ensure the following fields are correct and have data:

- Employee Status
- SSN
- First Name
- Middle Name
- Last Name
- Suffix
- Date of Birth
- Citizenship Status
- Business Email Address
- Business Phone Number
- Emergency Response Official **NEW!**
- LincPass Required **NEW!**
- Adjudication Information **NEW!**

The verification/update procedures are detailed in the sections A through C below, which are organized according to the EmpowHR user interface to help make the process as efficient as possible.

Section D includes information on how employees update the business email address and business phone number using the EmpowHR Self Service Module, both of which are required for the LincPass enrollment process.

It is important to note that all of these attributes can be entered with any regular PAR action, ie. **Name Chg from**. However, if updating the new HSPD-12 fields not part of a PAR action, it is important that the data is entered from the Employee Security Clearance menu item. This does not require a separate PAR action but only needs to be saved once complete. Instructions follow in Section A.

**Prerequisites:**

- You have access to and a user ID and password for USDA's EmpowHR system.
- You have background investigation (e.g., NACI) adjudication information for these employees, either from OPM records or USDA HR records.
- You have experience using EmpowHR, and have access to EmpowHR user guides and procedure manuals if needed.

**Note:** The screenshots used are from the EmpowHR test system. There may be slight variances in the EmpowHR production system you are using.

**A. PAR Processing**

**MENU ITEM: HR Processing**

**TAB: Personal Data**

1. From EmpowHR's left side menu, click **PAR Processing**, then click the link for **HR Processing**.
2. Use the search fields to locate the employee's record.
3. Click the **Personal Data** tab (see Figure 1). Verify the following fields have current and correct information:
  - Employee status (should be "Active")
  - SSN
  - Name (First, Middle, Last, Suffix)
  - Date of Birth
  - Citizenship Status\*



\*If Citizenship Status is specified as anything other than 1 for U.S. Citizen, the Citizenship Country must be selected in the field below.

The screenshot shows the 'Personal Data' tab in the EmpowHR system. At the top, the employee's name 'Ford, Lida' is displayed along with their EmpID (099381), Emp Rec# (0), and SSN (999-09-9361). Below this, the 'Personal Data' section includes the following fields: Effective Date (05/31/2007), Transaction# (Seq 1 1), PAR Status (Processed by Human Resources), NOA Code, Act Type (Data Change), Emp Status (Active), and SSN (999-09-9361). The Name section contains First (Lida), Middle, Last (Ford), Suffix, Name (Ford, Lida), and Alias Name. The Gender section has radio buttons for Male and Female (selected), and a dropdown for Handicap Code (No Handicap). The RNO is 'White, not of Hispanic origin'. The Date of Birth is 04/27/1962, and the Draft Status is 'Not Applicable'. The Citizenship Status is '1', and the Citizenship Country field is empty. At the bottom, there are buttons for Save, Return to Search, Previous tab, Next tab, Update/Display, and Correct History.

Figure 1. Verify information on the Personal Data tab

4. If any of the information is incorrect, missing, or needs updating, follow standard EmpowHR PAR Action Procedures for making the necessary changes and saving the record. For example, Name changes should be done according to the **Name Chg from** Action and Date of Birth or Citizenship Status changes should be done according to the **Data Change** Action.

**MENU ITEM: Employee Security Clearance**

5. From EmpowHR's left side menu click ►PAR Processing, then click the link for Employee Security Clearance.
6. Use the search fields to locate the employee's record.
7. In the Investigation block, click the **LincPass Required** checkbox (see Figure 2).

Procedures to Verify/Update Employee Records in EmpowHR

Figure 2. Update the Investigation section of the Security Info screen

8. You may optionally enter data in the Notes field. NOTE: If the employee has not completed his/her background investigation, the Employee's Submitting Office Number, Security Office Identifier and OPAC/ALC must also be entered. Disregard the Card Activation Information link.
9. If the Employee is an Emergency Response Official, designate this status by clicking the **Emergency Response Official** checkbox (see Figure 2 above).
10. Save the updates by clicking the **Save** button.

### C. PAR Processing

#### Adjudication Information

11. From EmpowHR's left side menu, click **PAR Processing**, then click the link for Adjudication Information (see Figure 6). This is a new option created to accommodate HSPD-12 requirements.

Figure 6. New Adjudication information option for HSPD-12

- Search for the Employee and in the Adjudication tab, fill in the Investigation Type, Status, and Notes fields (see Figure 7). The Adjudication Date and Adjudicator OprID will be populated by the system.

Investigation Type	Status	Adjudication Date	Adjudicator OprID	Notes
1   NACI	Approved	05/31/2007	DR123456	Emp +15 yrs - Defaulted

Figure 7. Enter Adjudication results information

- Investigation Type:** Use the droplist to select the appropriate Investigation Type the employee has completed. If the employees completed background investigation is not in the droplist because it is higher than a NACI, select the "NACI" option because that is the highest background investigation level that HSPD-12 is concerned with.

**Note:** The contents of the droplist and the instructions may change for the full rollout.

- Status:** Use the droplist to select the "Approved" option for confirmed background investigation
- Notes:** Reference This field can be used to enter in the true adjudicator name and actual adjudication date.
- Adjudication Date and Adjudicator OprID:** These two fields are populated by the system

#### D. Employee Self Service – Personal Information

**Note:** This section is only for EmpowHR employee users who need to update their business email and business phone information in the EmpowHR self service module.

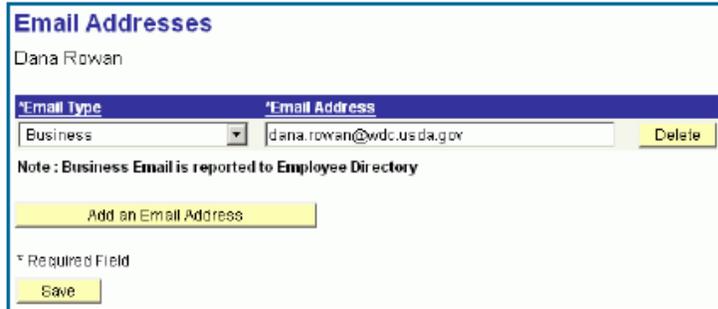
##### Email Addresses

- From EmpowHR's left side menu, click ►Employee Self Service, then click the Personal Information link (see Figure 8).

Figure 8. Employee Self Service options

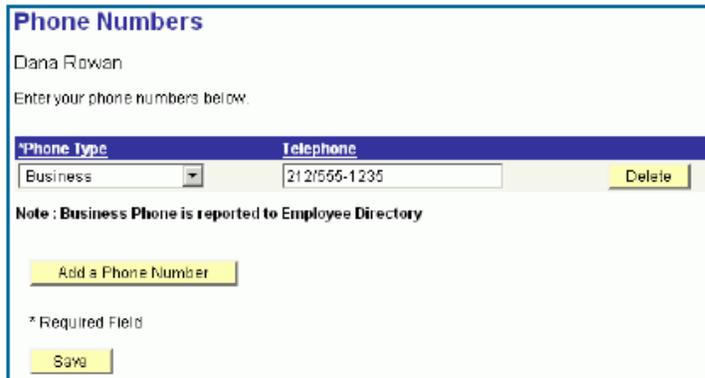
**Procedures to Verify/Update Employee Records in EmpowHR**

14. To verify/update your business email address, click the [Email Addresses](#) link.
15. In the *Email Type* column, use the droplist to select "**Business**," then enter your current business email address in the Email Address field (see Figure 9). Click the **Save** button.



*Figure 9. Update your own business email address*

16. From EmpowHR's left side menu, click the [Phone Numbers](#) link.
17. In the Phone Type column, use the use the droplist to select "**Business**," then enter your current business phone number in the Telephone field (see Figure 10). Click the **Save** button.



*Figure 9. Update your business phone number*

