

# **USDA HSPD-12 Security Officer Guide**

Prepared for



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

**Version 2.0**

**August 25, 2008**



## Revision Information

Version	Date	Revision Notes
1.0	6/5/2008	Initial Draft
2.0	8/25/2008	Updated screen shots, changed verbiage from "revoked" to "terminated"



## Table of Contents

<b>Section 1</b>	<b>Introduction.....</b>	<b>1</b>
<b>Section 2</b>	<b>Clearing Flagged Records .....</b>	<b>2</b>
2.1	About Flagged Records .....	2
2.2	Clearing I-9 Document Referral Flags .....	2
2.3	Clearing Biometric Duplicate Flags .....	8
<b>Section 3</b>	<b>Changing LincPass Status .....</b>	<b>14</b>
3.1	Suspending a LincPass .....	14
3.2	Reactivating a LincPass .....	16
3.3	Revoking a LincPass .....	17
<b>Section 4</b>	<b>Lost/Found LincPasses .....</b>	<b>19</b>
4.1	Lost LincPass .....	19
4.2	Found LincPass .....	21
4.3	Policies.....	22
<b>Section 5</b>	<b>LincPass Destruction.....</b>	<b>24</b>
<b>Section 6</b>	<b>LincPass Handling .....</b>	<b>24</b>
<b>Section 7</b>	<b>Applicant Status Report.....</b>	<b>24</b>

## Section 1 Introduction

This document serves as a guide to the HSPD-12 Security Officer processes and procedures. It details the role's major responsibilities and provides instructions on performing various HSPD-12 Security Officer duties. Specifically this document covers:

- Clearing Flagged Records
  - Clearing I-9 Document Referral Flags
  - Clearing Biometric Duplicate Flags
- Changing LincPass Status
- LincPass Destruction
- Handing LincPasses
- Using the Applicant Status Report

Before proceeding, please make sure that you have met all the pre-requisites for performing HSPD-12 Security Officer Duties:

1. Sponsored in the USAccess system
2. Successfully completed the USAccess Security Officer training
3. Your Agency Role Administrator has designated you as a Security Officer in USAccess
4. Received your USAccess user ID and password

**NOTE:** Both a Sponsor and Security Officer have the capability to mark a LincPass destroyed in USAccess. Due to this, each agency has the flexibility to build a business process model where either the Sponsor or Security Officer is responsible for taking possession of suspended/terminated LincPasses and destroying them. Agencies should design the process to best fit the logistical needs within their agencies. This document is built on a model where the Security Officer is responsible for these tasks.

## Clearing Flagged Records

### 1.1 *About Flagged Records*

A pre-issuance duty of the HSPD-12 Security Officer is to review Applicant records that have been flagged during the Enrollment process. This system flag is in place so the Applicant cannot receive a LincPass or continue through the USAccess Credentialing process without Security Officer approval once they are flagged for review. Applicant records can be flagged for I9 document referrals and/or biometric duplicates. For either flag, it is the Security Officer's responsibility to review these records in USAccess and then clear the flag if the conditions warrant.

#### 1.1.1 Document Referral Flags

During the Enrollment process, a Registrar marks documents for more validation when a source identity document looks fraudulent or tampered with. The Registrar may also flag the record if the Applicant indicates in some way that they are not who they say they are.

Previously, a Security Officer had to review and clear flagged records on-site at an Enrollment Station. Now, this functionality has been integrated into the USAccess Security Officer Web Portal.

#### 1.1.2 Biometric Duplicate Flags

During the Enrollment process, the system may flag an Applicant's record if their fingerprints match closely to fingerprints already in the system. This check is in place to ensure that an Applicant who has already registered does not try to register again under a separate identity. The opposite holds true in re-enrollment situations (i.e. LincPass Renewals or Reissues). The system will flag applicant records if it cannot find a previous biometric match for the Applicant.

## 1.2 *Clearing I-9 Document Referral Flags*

### 1.2.1 Generate Applicant Status Report

**Step 1.** Generate an Applicant Status report and save it as an excel file on your computer.

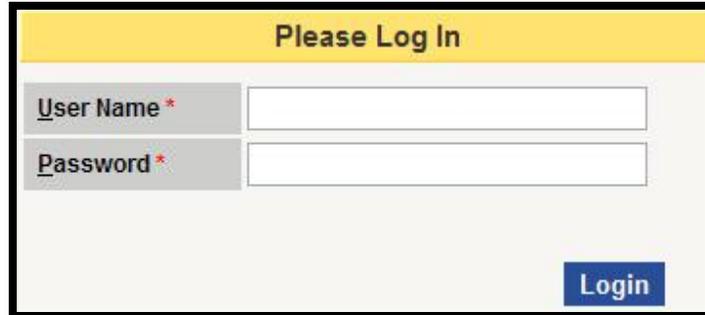
**Step 2.** Filter the report to show only Applicants in your agency who have a flag on their record

- Document Referrals: "DocumentReferral" column = "Yes"
- Biometric Duplicates: "DuplicateCheckPending" column = "Duplicate Found"

Please see the "Using the Applicant Status Report" guide on the USDA HSPD-12 website's ["Training"](#) page if you need more details on running the Applicant Status Report.

### 1.2.2 Review the Applicant's Record

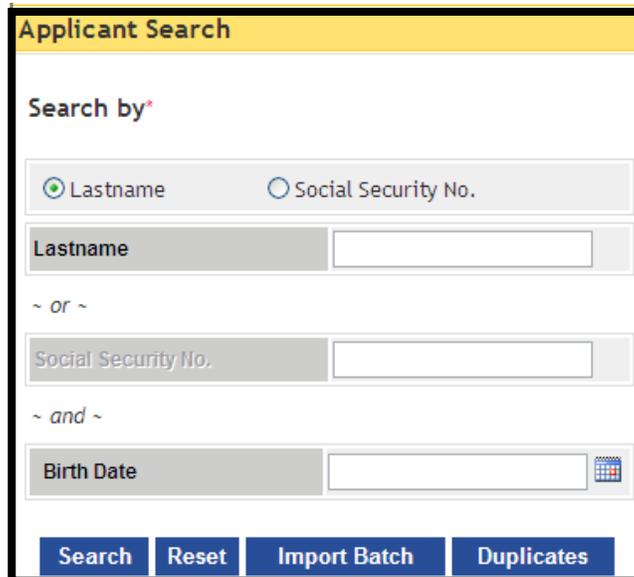
**Step 1.** Log into the USAccess Security Officer web portal (<https://gsa.identitymsp.com/ASSUREDIDENTITYPORTAL>) with your USAccess user name and password.



The login screen features a yellow header with the text "Please Log In". Below the header are two input fields: "User Name\*" and "Password\*", each with a corresponding text box. A blue "Login" button is positioned at the bottom right of the form.

Figure 1: SO Portal Login Screen

**Step 2.** Search for the flagged Applicant by entering their SSN or Birth date and the Last Name and then clicking the **Search** button.



The search screen has a yellow header "Applicant Search". Under "Search by\*", there are two radio buttons: "Lastname" (selected) and "Social Security No.". Below these are three input fields: "Lastname", "Social Security No.", and "Birth Date" (with a calendar icon). At the bottom are four buttons: "Search", "Reset", "Import Batch", and "Duplicates".

Figure 2: Applicant Search Screen

**Step 3.** When the Applicant's record displays, click the **View Advanced** button.

ID	Last Name	First Name	Birth Date	Social Security	Email	Status	
1000020640	ABADIE	CONNIE	11/25/1956	xxx-xx-5019	CONNIE.ABADIE@USDA.GOV	REGISTERED	<b>View Advanced</b>

Figure 3: Applicant Record

**Step 4.** The **Card Status** screen displays, however since a LincPass has not been issued yet for this Applicant, the Card Status screen will display with no records found. Select the **Document Validation** tab.

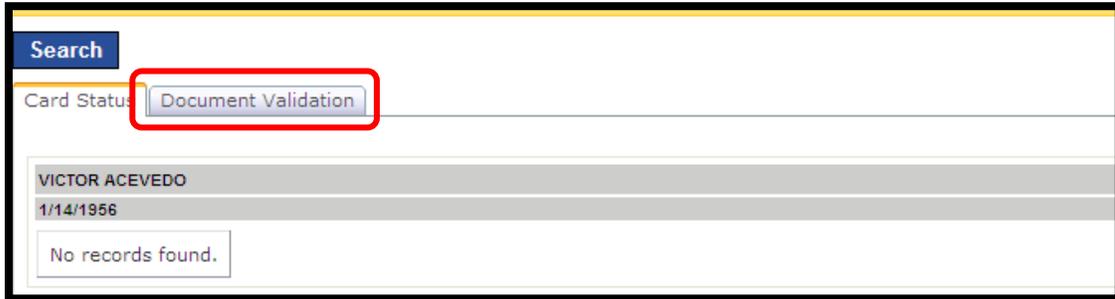


Figure 4: Card Status Screen

**Step 5.** The **Document Validation** screen appears. Use the **Biographic Data**, **Address Data**, and **Photo** tabs to review the Applicant's record.

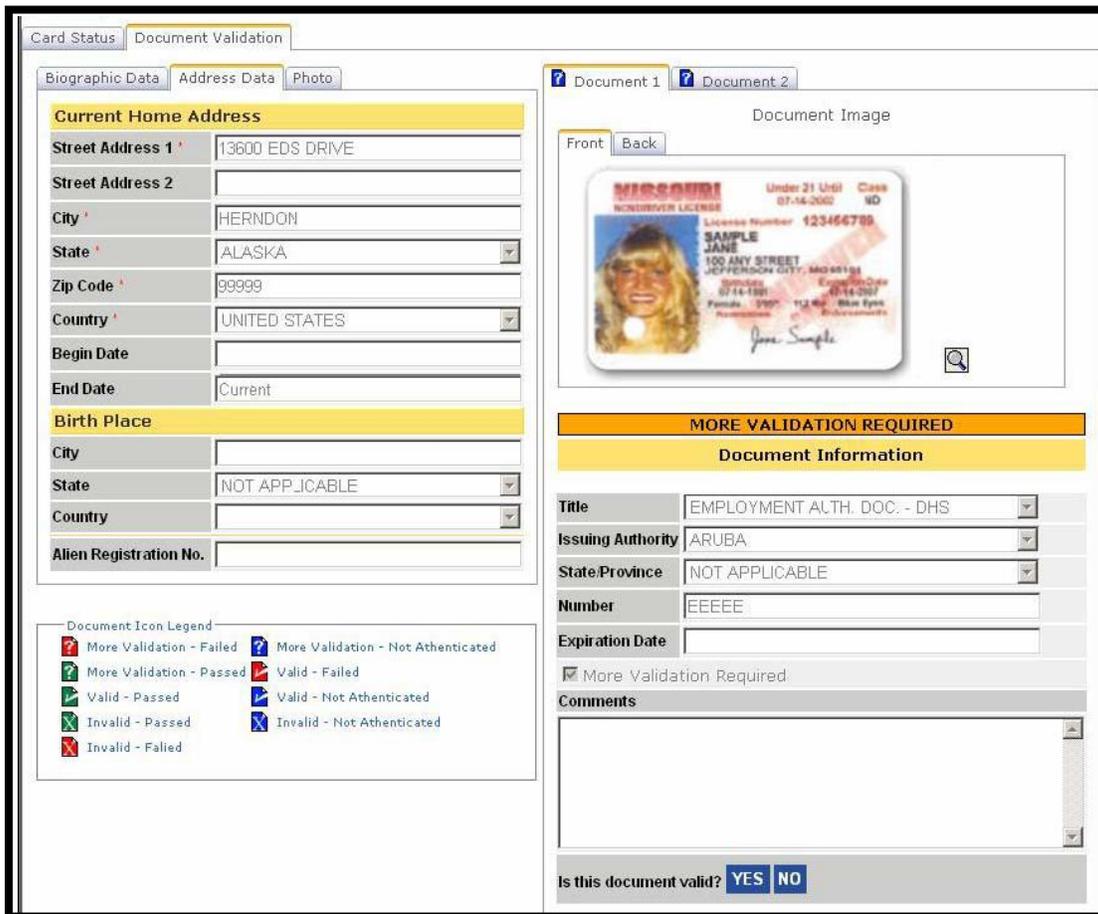


Figure 5: Document Validation Screen

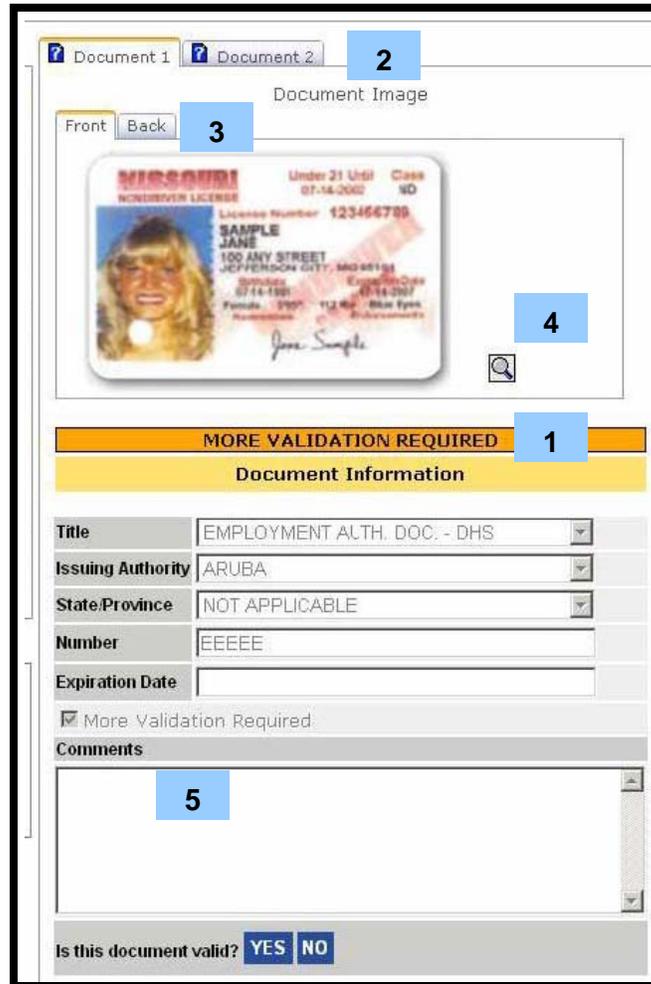


Figure 6: Document Validation Screen

**Step 6.** Documents marked for more validation are labeled with an orange **More Validation Required** sign (#1).

Use the **Document** (#2) tab to review the documents that were referred for more validation.

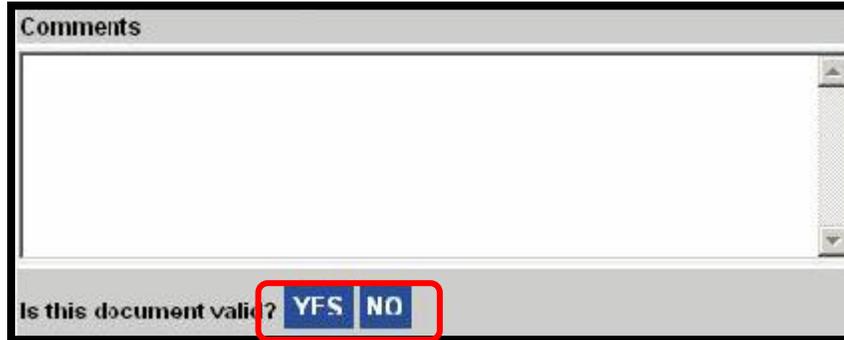
Use the **Front** and **Back** tabs (#3) to view both sides of the document.

Click the magnifying glass (#4) to enlarge the document images

Registrar comments will display in the **Comments** field (#5)

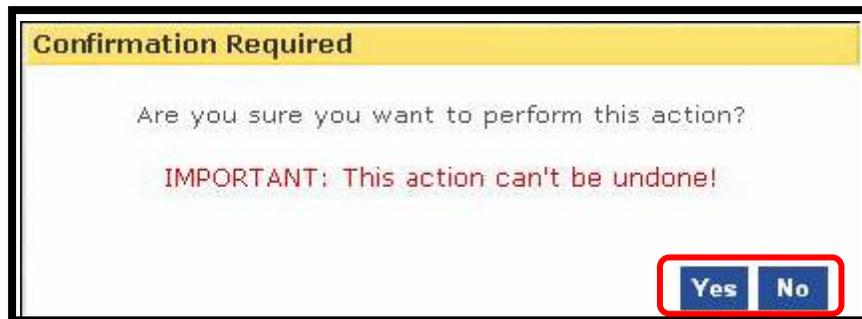
**Step 7.** Icons on the **Document** tabs indicate how the document was scanned and marked for more validation. See explanation of icons in the next section.

**Step 8.** After reviewing the document, click **Yes** to mark the document as valid or **No** to mark the document as invalid.



*Figure 7: Document Validation*

**Step 9.** The “Confirmation Required” message reminds you that the action you are taking will immediately go into the database and you will not be able to change it. Click the **Yes** button if you are sure about your decision; otherwise click the **No** button to revisit the Applicant’s record.



*Figure 8: Confirmation Screen*

**NOTE:** Applicants whose records are marked invalid by the Security Officer will not receive a LincPass. The process will stop at this point.

### 1.2.3 Document Flag Icons

Icon	Label	Description
	More Validation - Failed	License failed the AssureTec scan and was marked for more validation
	More Validation – Passed	License passed the AssureTec scan and was marked for more validation
	More Validation – Not Authenticated	The document was not scanned in the AssureTec scanner and was marked for more validation
	Invalid – Failed	Indicates the Security Officer has marked the Failed document invalid
	Invalid – Passed	Indicates the Security Officer has marked the Passed document invalid
	Invalid – Not Authenticated	Indicates the Security Officer has marked the Not Authenticated document invalid
	Valid – Failed	Indicates the Security Officer has marked the Failed document valid
	Valid - Passed	Indicates the Security Officer has marked the Passed document valid
	Valid – Not Authenticated	Indicates the Security Officer has marked the Not Authenticated document valid

If the Security Officer determines the document is valid, the “?” icon is replaced with the appropriate checkmark icon, depending on the document’s status with being scanned in the AssureTec scanner.

If the Security Officer decides the document is not valid, the “?” icon is replaced with the appropriate “X” icon, depending on the document’s status with being scanned in the AssureTec scanner.

### 1.3 Clearing Biometric Duplicate Flags

The second type of review is of possible duplicate records. This flag may be placed by the USAccess System when the Applicant enrolls and a new enrollment record is created in USAccess. The System compares the fingerprints in the new record with fingerprints in all of the other records in the system.

If the record is for a new Applicant, there should be no previous record in the system. If a match is found, a link to the match is placed in the Security Officer’s **Match Results** queue for review. If the new record is a re-enrollment, a previous record should be found in the system for the Applicant. If no record is found, or if there is a fingerprint match, but the biographical information does not match, a link is placed in the Security Officer’s **Match Results** queue for review.

#### 1.3.1 First Time Enrollment Biometric Duplicate

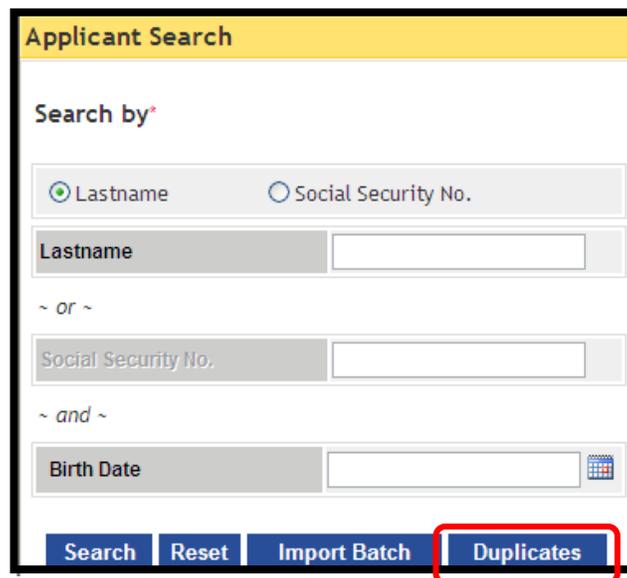


Figure 9: Applicant Search Screen

**Step 1.** From the Applicant Search page, click on the **Duplicates** button

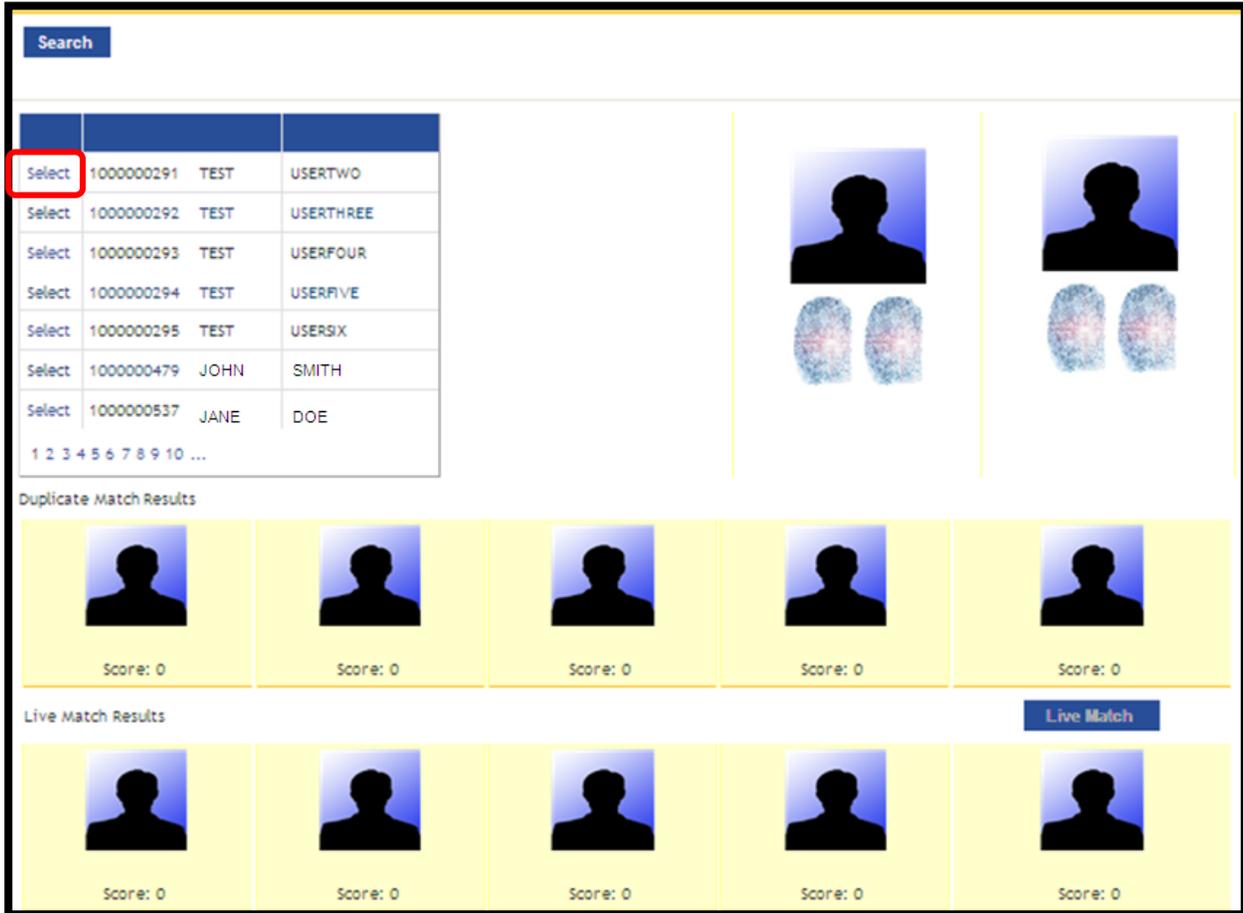


Figure 10: Duplicates Screen

**Step 2 .** The **Security Officer Duplicates** page will display. The oldest entry is at the top of the list on page 1 and the newest is at the bottom of the list on the last page. Click on the **Select** link next to the record to review it.

Select	1000003456	TEST	USERNINE
Select	1000003457	TEST	USERTEN
Select	1000008776	LAURIE	SMITH
Select	1000008793	OLA	DOE
Select	1000010827	EVELYN	JACKSON
Select	1000011567	DENISE	KENT
Select	1000011833	JAMES	WAYNE

1 2 3 4 5 6 7 8 9 10 ...

Duplicate Match Results

Duplicate?

#1: 1000011567 DENISE KENT UNITED STATES 8/27/1952

#2: 1000011567 DENISE 'KENT UNITED STATES 8/27/1952

#3: Duplicate? YES NO

#4: 1000011567 Score: 644.122

Live Match Results

Score: 0

Score: 0

Score: 0

Score: 0

Score: 0

Live Match

Figure 11: Duplicates

**Step 3.** The page will display several pieces of information:

- The Applicant (#1)
- The potential duplicate (#2)
- Duplicate decision buttons (#3)
- The match score (#4)

The system will alert you to a possible duplicate record and will provide a photo and match score to help you decide if there is a duplicate. The match score reflects how closely the fingerprints of the new enrollee match those of enrollees already in the system. A score of 5 or higher indicates the possibility of a fingerprint match. When the score is very high, for example 644 as you see on this page, it is very likely the same person. For that reason, even though the photos are different, you would probably consider this a match and investigate further. The closest match is displayed next to the enrollee and above the rows of other possible matching documents.

Duplicate? YES NO

Select	1000003456	TEST	USERNINE
Select	1000003457	TEST	USERTEN
Select	1000008776	LAURIE	SMITH
Select	1000008793	OLA	DOE
Select	1000010827	EVELYN	JACKSON
Select	1000011567	DENISE	KENT
Select	1000011833	JAMES	WAYNE

1000011567  
DENISE KENT  
UNITED STATES  
8/27/1952

1000011567  
DENISE 'KENT  
UNITED STATES  
8/27/1952

Duplicate Match Results

1000011567  
Score: 644.122

Select

1000039082  
Score: 1.159

Select

1000000589  
Score: 1.157

Select

1000001208  
Score: 1.041

Select

1000037454  
Score: 0.978

Select

Live Match Results Live Match

Figure 12: Marking the Duplicate

**Step 4.** For this enrollee, click the **YES** button to confirm the flag; otherwise click the **NO** button to clear the flag.

**NOTE:** Before you make your decision, you might want to update the match results. When you click the link besides the enrollee's name to the view the match results, you will see the results from the day the duplicate search was performed. To see up-to-date results, click the **Live Match** button.

**NOTE:** Be very sure you are making the correct determination as it cannot be undone once submitted. Once the duplicate is confirmed the LincPass issuance process will stop for this Applicant.

### 1.3.2 Re-enrollment Biometric Duplicate

For a re-enrollment, you would expect to find a duplicate record since the Applicant is being re-enrolled. If the system finds a match, but the biographical data is different, it will return the match as a duplicate for your review.

Conversely, if no records exceed the threshold of 5, there is no duplicate record for this enrollee. The duplicate will be listed for your review since this could be someone trying to re-enroll under a different name.

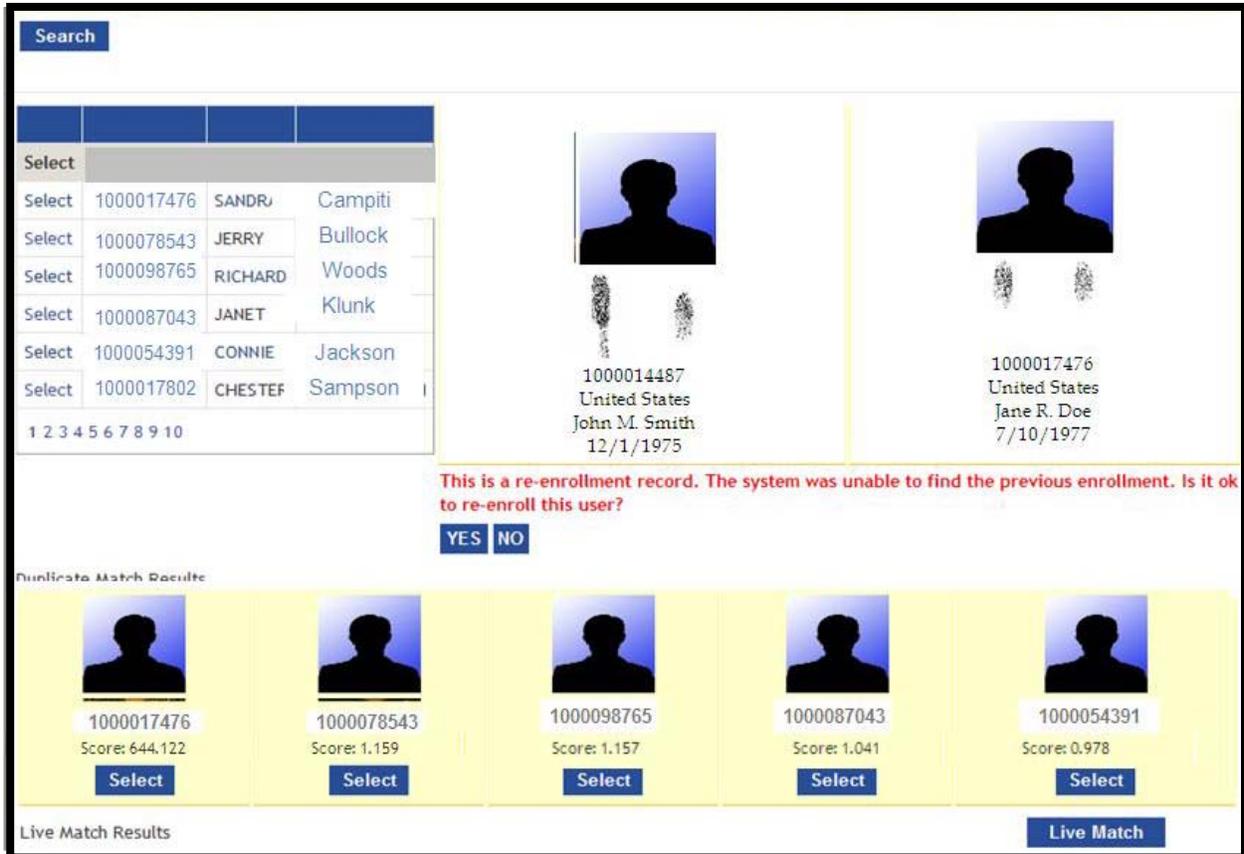


Figure 13: Re-enrollment

**Step 1.** The Applicant and Potential duplicate display along with Re-enrollment decision buttons. Even though the match score is very high, there is good reason to believe these are not duplicates. The name, birth date, and enrollment number are different. It is your discretion whether this is the same or a different person.



Figure 14: Deny Re-Enrollment

**Step 2.** Click the **No** button to confirm this duplicate flag. Click the **Yes** button to clear the flag.

**NOTE:** Be very sure you are making the correct determination as it cannot be undone once submitted. Once the duplicate is confirmed the LincPass issuance process will stop for this Applicant.

## Section 2 Changing LincPass Status

The Security Officer has the ability to change the status of LincPass independently of the Applicant’s employment status. This may be necessary when someone loses a LincPass, goes on leave for a temporary period of time, is involved in a security event, or for any other event requiring a status change as defined by agency policies. The Security Officer has the capability to completely terminate a LincPass, suspend the LincPass for a period of time, or reactivate it after suspending it.

### 2.1 Suspending a LincPass

Certain conditions may warrant suspending the LincPass for a period of time. Suspending it turns the LincPass certificates off without terminating the LincPass completely so that it can be used again after being reactivated.

**Step 1.** Log into the USAccess Security Officer web portal (<https://gsa.identitymsp.com/ASSUREDIDENTITYPORTAL>) with your USAccess user name and password.

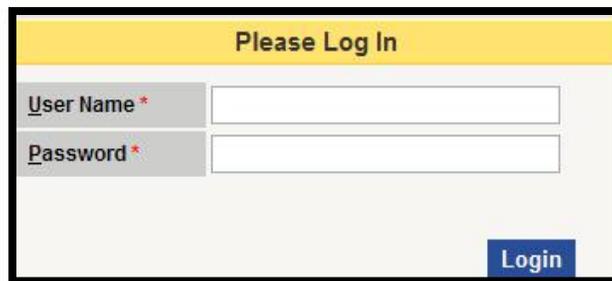


Figure 15: SO Portal Login Screen

**Step 2.** Search for the flagged Applicant by entering their SSN or Birth date and the Last Name and then clicking the **Search** button.

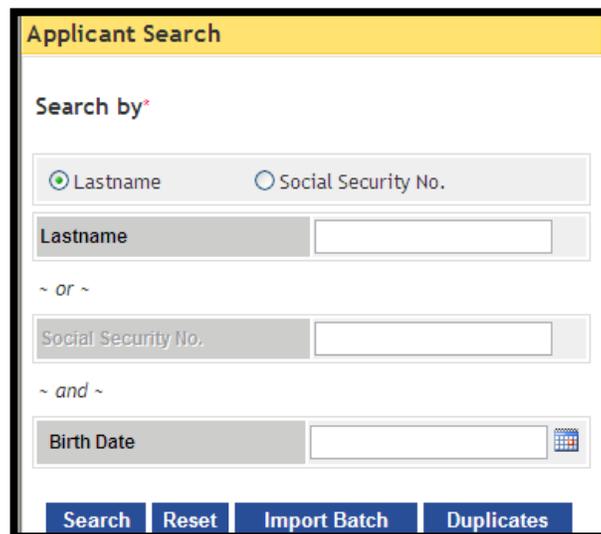


Figure 16: Applicant Search Screen

ID	Last Name	First Name	Birth Date	Social Security	Email	Status	
1000001234	SMITH	JANE	1/1/1970	xxx-xx-1234	JANE.SMITH@USDA.GOV	REGISTERED	<a href="#">View Advanced</a>

Figure 17: Applicant Record

**Step 3.** When the Applicant’s record displays, click the **View Advanced** button.

Search						
Card Status <a href="#">Document Validation</a>						
JANE SMITH						
1/1/1970						
PIV Card Serial Nbr	PIV Card Status	Sponsor Agency	Suspend	Reactivate	Terminate	Destroyed
2050500001145678912	ACTIVATED	DEPARTMENT OF AGRICULTURE	<a href="#">Suspend</a>		<a href="#">Terminate</a>	

Figure 18: Card Status Screen

**Step 4.** The Security Officer portal appears with the **Suspend** and **Terminate** buttons present. Note the **Reactivate** button is not available until a LincPass is suspended. Click the **Suspend** button to suspend the LincPass.

Search						
Card Status <a href="#">Document Validation</a>						
JANE SMITH						
3/25/1962						
PIV Card Serial Nbr	PIV Card Status	Sponsor Agency	Suspend	Reactivate	Terminate	Destroyed
205000112778D452E45	SUSPENDED	DEPARTMENT OF AGRICULTURE		<a href="#">Reactivate</a>	<a href="#">Terminate</a>	

Figure 19: Suspended LincPass

**Step 5.** The LincPass is now suspended and the Reactive button is now available. Collect the LincPass for storage until it is either reactivated or revoked.

**NOTE:** An individual must retain their affiliation with the federal government while inactive. If they are terminated, then the LincPass will be terminated once the employment status change is sent to USAccess.

## 2.2 Reactivating a LincPass

The Security Officer can reactivate a LincPass that has previously been suspended by a Security Officer. Please note that if the employment status is suspended, the LincPass cannot be reactivated by the Security Officer.

PIV Card Serial Nbr	PIV Card Status	Sponsor Agency	Suspend	Reactivate	Terminate	Destroyed
205000112778D452E45	SUSPENDED	DEPARTMENT OF AGRICULTURE		Reactivate	Terminate	

Figure 20: Card Status Screen

**Step 1.** Follow steps 1-3 in section 2.1 in order to access the card status screen for this cardholder.

**Step 2.** Click the **Reactivate** button.

PIV Card Serial Nbr	PIV Card Status	Sponsor Agency	Suspend	Reactivate	Terminate	Destroyed
2050500001145678912	ACTIVATED	DEPARTMENT OF AGRICULTURE	Suspend		Terminate	

Figure 21: Reactivated LincPass

**Step 3.** The LincPass has been successfully reactivated. Return the LincPass to the cardholder.

## 2.3 Terminating a LincPass

The Security Officer can terminate a LincPass thereby permanently revoking the LincPass and the certificates. The LincPass can never be turned back “on” again and the cardholder will need to be reissued a new one should one be needed. There may be several reasons to terminate a LincPass; see section 2.3.2 for details

### 2.3.1 Terminating a LincPass in USAccess

PIV Card Serial Nbr	PIV Card Status	Sponsor Agency	Suspend	Reactivate	Terminate	Destroyed
2050500001145678912	ACTIVATED	DEPARTMENT OF AGRICULTURE	Suspend		Terminate	

Figure 22: Card Status Screen

**Step 1.** Follow steps 1-3 in section 2.1 in order to access the card status screen for this cardholder.

**Step 2.** Click the **Terminate** button.

PIV Card Serial Nbr	PIV Card Status	Sponsor Agency	Suspend	Reactivate	Terminate	Destroyed
20505000115879745C3	TERMINATED	DEPARTMENT OF AGRICULTURE				Destroy

Figure 23: Terminated LincPass

**Step 3.** The LincPass has now been terminated and only the **Destroy** button is present.

At this point the LincPass should be collected from the Applicant, physically destroyed and then marked as such in USAccess by either the Sponsor or the Security Officer. See section 4 for information on destroying the LincPass.

### **2.3.2 Termination Reasons**

Below are some of the most common reasons to terminate a LincPass. There may be other situations that arise that require termination as well.

Provisional LincPass: If a LincPass was issued provisionally after a favorable fingerprint check adjudication, it may need to be terminated if there is an unfavorable NACI adjudication.

Defective LincPasses: An Activator will return LincPasses with manufacturer defects; you must then terminate these LincPasses.

Lost or Stolen LincPass: Once the determination has been made that the LincPass is permanently lost or known to be stolen, the Security Officer should terminate it

**NOTE:** When you terminate a LincPass, you must collect it from the employee (if available) and destroy the card according to the processes in the LincPass Destruction Guide.

### Section 3 Lost/Found LincPasses

Whenever an cardholder loses their LincPass or one has been found, the Security Officer must take possession of the LincPass and review the status of the LincPass. The following workflows detail the process for handing lost and/or found LincPasses.

#### 3.1 Lost LincPass

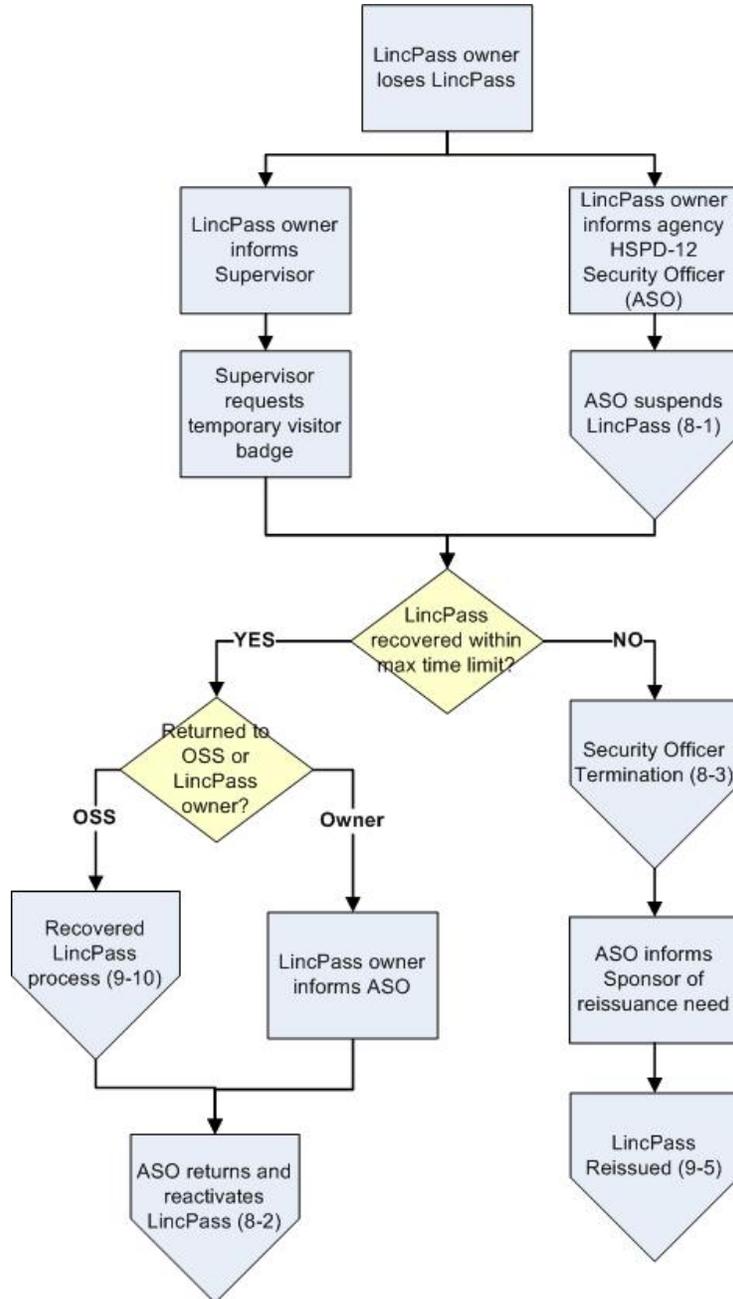


Figure 24: Lost LincPass

1. The LincPass owner loses possession of their LincPass.
2. The LincPass owner immediately informs their agency's HSPD-12 Security Officer (ASO) who will record it in a Lost LincPass log.
3. The ASO suspends the LincPass in USAccess.
4. Meanwhile, the LincPass owner informs their supervisor that they have lost their LincPass.
5. The Supervisor requests a temporary visitor badge for the LincPass owner from the appropriate local physical security personnel.
6. If the LincPass is not recovered within 72 hours of being reported lost, do the following; otherwise go to step 7.
  - a. The Security Officer terminates the LincPass.
  - b. The Sponsor initiates a reissuance request for the LincPass owner (Termination contained within Reissuance process).
  - c. The LincPass owner re-enrolls using the standard Enrollment process.
7. If the LincPass is returned to the owner directly within the maximum time limit from being reported lost do the following; otherwise go to step 8.
  - a. LincPass owner informs ASO that they have received their LincPass
  - b. Go to step 10
8. The LincPass is found by OSS, logged, and then returned to the ASO.
9. The ASO returns the LincPass to the owner and reactivates it in USAccess.

### 3.2 Recovered LincPass

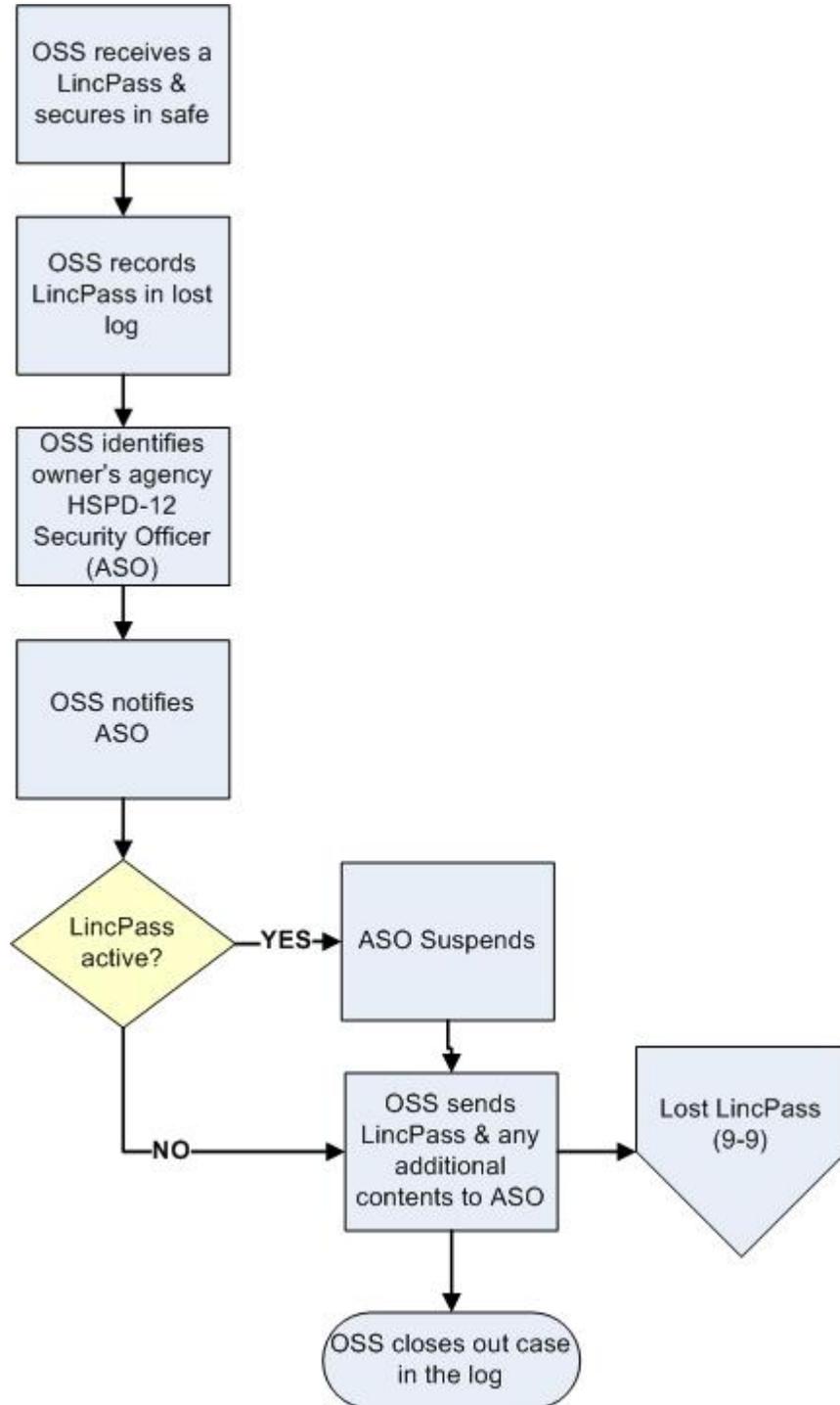


Figure 25: Found LincPass

1. OSS receives a lost LincPass and securely stores it and any additional contents returned with it (i.e. safe or other secure container).
2. OSS records a new log entry for the LincPass (including cataloguing any additional contents received with the LincPass) in the log.
3. OSS identifies the LincPass owner's agency HSPD-12 Security Officer (ASO).
4. OSS informs the ASO that a LincPass from their agency has been recovered.
5. The ASO checks the LincPass status. If the LincPass is Active, the ASO suspends it; otherwise go to step 6.
6. OSS sends the LincPass and any additional contents to the ASO.
7. OSS closes out the item in the log.
8. The ASO follows the Lost LincPass process from step 6.

### **3.3 Policies**

#### **3.3.1 Logging of LincPasses**

Both the Agency Security Officer and OSS will keep a recorded log of all lost and recovered LincPasses and the actions taken upon them. This log should allow for documenting the following details and must be updated as events occur:

- LincPass Owner
- LincPass Owner's Agency Security Officer
- OSS officer
- Additional contents received with the LincPass
- Events and dates associated with actions taken

#### **3.3.2 Notification of Lost/Recovered LincPass**

LincPass owners must inform their Agency Security Officer within 72 hours when they realize their LincPass is lost. In accordance with DM4620-XX, Chapter 2, Section 6, the LincPass owner will also inform their Supervisor so that the Supervisor can request a temporary visitor badge from the local physical security personnel. If a LincPass is recovered by OSS, they will identify and notify the LincPass owner's Agency Security Officer within 1 business day.

#### **3.3.3 Lost LincPass Status Review**

Once the Agency Security Officer has been notified by the owner of a lost LincPass, they will immediately suspend the LincPass to prevent security issues. The LincPass can remain suspended up to a maximum of 5 business days; however the Agency can terminate the LincPass at any time during this 5 day period. After the 5 business day limit has expired, it must be terminated by the Agency Security Officer.

#### **3.3.4 Recovered LincPass Status Review**

Once OSS has recovered a LincPass, they will inform the owner's Agency Security Officer. The Agency Security Officer must review the status of the LincPass in USAccess. If the LincPass is still active, they should suspend it within 1 business day until it is returned. If it is already suspended or terminated, they do not need to take action on the status.

### **3.3.5 Physical Return of Recovered LincPass**

OSS must send the suspended LincPass (and any additional contents) to the Agency Security Officer via registered mail, or deliver in person, within 2 business days of receiving the LincPass. The Security Officer must ensure that the LincPass is not returned or reactivated until the owner presents a photo based I-9 document in person to the Security Officer to verify their ownership of the LincPass.

### **3.3.6 Destruction of Terminated Recovered LincPass**

If the LincPass has already been terminated prior to recovery, the Agency Security Officer will destroy the LincPass within 18 hours of receipt per FIPS201-1 requirement and according to the LincPass Destruction guidelines.

### **3.3.7 Reissuance of Terminated LincPass**

Once the LincPass has been terminated, a new LincPass will need to be reissued and the temporary visitor badge will be surrendered to the appropriate physical security personnel after the new LincPass has been issued and activated. The Security Officer must inform the Sponsor within 1 business day that a LincPass has been terminated and a reissuance is required. The Sponsor will reissue the LincPass using the standard Reissuance process within 1 business day.

## Section 4 LincPass Destruction

Whenever a LincPass is terminated either by the Security Officer, by the Sponsor due to an employment termination, or whenever a cardholder obtains a new one through a reprint or reissue the LincPass must be collected and properly destroyed.

Please see the “LincPass Destruction Guide” (<http://hspd12.usda.gov/training.html>) for detailed guidance on destroying the LincPass.

## Section 5 LincPass Handling

It is important that any time a Security Officer takes possession of or gives up possession of the LincPass, that they document the event in some manner. The goal of the log sheet is to provide an audit trail for when you obtain a LincPass and when you relinquish possession of the LincPass.

An example log sheet is provided below:

Owner, Contents, Agency	Date/Method LincPass Obtained	LincPass Status	Recorded By	Owner’s Agency SO	Date Owner’s SO Notified	Date/Method LincPass Sent	Comments

As a Security Officer you may need to either send or receive a LincPass in situations when it has been lost and/or found or when the card has been delivered to a location other than where the cardholder works and they need it shipped to their location.

## Section 6 Applicant Status Report

The Security Officer is one of the roles that can access the USAccess Applicant Status report. This report is a list of each USDA applicant currently in the USAccess system. It details the Applicant’s progress through the issuance process and it is a valuable status tracking tool.

Note: The Applicant Status Report contains PII information and therefore it should not be distributed to non-USAccess Role Holders.

Please see the “Applicant Status Report Guide” (<http://hspd12.usda.gov/training.html>) for detailed guidance on using the Applicant Status Report.