

For: FFAS Employees

LincPass Certificate Expiration

Approved by: Deputy Administrator, Management



1 Overview

A Background

LincPass is USDA’s initiative that was developed to meet the guidelines of Homeland Security Presidential Directive (HSPD)-12 that requires Federal agencies to produce and issue Personal Identity Verification (PIV)-compliant credentials to employees. The LincPass badge provides USDA employees with an easily recognizable way to identify themselves, access IT equipment, and trust the identity of other HSPD-12 credential holders. USDA began issuing LincPass to their employees in 2007.

Each LincPass carries 2 expiration dates separate from each other, 1 date for the badge and 1 date for the certificate that supports the badge. The badge expiration date is shown on the top-right corner of the badge and has a 5-year expiration from date of issuance. The gold certificate, located in the lower-center of the card, does **not** show an actual expiration date, but instead this date is maintained in a database under the USAccess program. The certificate expires 3 years from issuance. USDA employees are notified by e-mail at least 90 calendar days before their certificate expiration date that their certificate is about to expire.

B Purpose

This notice informs FFAS employees that:

- an automatically generated reminder e-mail will be sent directly to each employee whose LincPass certificate is about to expire
- each employee is responsible for updating or rekeying their LincPass certificate **before** it expires using the guidelines in this notice
- failure to update their LincPass certificate expiration at a fixed or light activation station will result in the LincPass badge being terminated and will require the employee to re-enroll.

Disposal Date September 1, 2011	Distribution All FAS, FSA, and RMA employees; State Offices relay to County Offices
---	---

2 Certificate Expiration Notification

A Certificate Expirations

LincPass certificates have a 3-year expiration date contained in the encoded data. Each time a LincPass is re-issued, this 3-year term is refreshed. LincPass's that have been reprinted, because of card damage or defect, do **not** begin a new 3-year term.

B Notification Reminders

System-generated e-mails will be automatically sent to each employee that possesses a LincPass **before** their LincPass certificate expires, reminding them that their certificate is about to expire and describing the actions required by the recipient to rekey the certificate. Reminder e-mails are sent to employees at the following intervals when their certificates are about to expire:

- 90 calendar days before expiration
- 60 calendar days before expiration
- 30 calendar days before expiration
- 15 calendar days before expiration
- 7 calendar days before expiration.

Note: LincPass holders **cannot** begin their certificate rekeying process until they receive the first reminder e-mail. The actual date of certificate expiration will be shown on the reminder e-mail.

LincPass holders will continue to receive the reminder e-mails until their LincPass certificate is rekeyed. If a holder attempted to rekey their certificate and they still receive the reminder e-mail, their attempt was **not** successful and they should redo the process until successful.

C Notification Sender

Automatically generated LincPass certificate reminder e-mails will be sent to each employee that possesses a LincPass from **HSPD12Admin@identitymsp.com**.

The subject line for the reminder e-mail will show, "**Subject:** USAccess - ACTION REQUIRED: Update Your USAccess Credential (PIV Card)".

Note: Reminder e-mails have been, at times, inadvertently sent directly to the recipients "Junk E-mail" box, instead of their "Inbox". Employees shall make every effort to ensure that this reminder e-mail is **not** mistakenly deleted when removing junk e-mails.

3 Certificate Rekeying Instructions

A National, State, and County Office Actions

Instructions for rekeying LincPass certificates are the same for all FFAS employees. State and County Office employees may elect to use the Lite Activation Sites for rekeying their LincPass certificates after these locations become available.

See Exhibit 1 for rekeying instructions for LincPass certificates.

B Certificates Not Rekeyed Before Their Expiration Date

Employees shall **not** allow their LincPass certificates to expire. If expiration occurs, the LincPass will be automatically terminated by the USAccess and the employee will have to enroll for a new LincPass. The enrollment process means the employee must visit an enrollment center to present their identification documents, submit fingerprints, and have their picture re-taken. They **must** then wait for their new credential to be printed, delivered, and activated. During this time, the employee may **not** be able to log on to their work computer or gain access to Government buildings, if they currently use their USAccess credential for these purposes. **In addition, this inaction will force the Agency to incur a significant cost.**

4 State HSPD-12 Sponsors Actions

A Sponsors Action

State HSPD-12 sponsors can access Certificate Expiration Report for their State and county employees through the GSA Reports Portal. To access this report, after signing onto the site, sponsors shall select “**report viewer**”, then select “**Certificate Expiration Report.rpt**”. Reports can be generated to show certificate expiration of up to 180 calendar days of expiration, as well as employees with expired certificates. The report can be sorted to remove data **not** associated with their State.

B Contacts

Direct questions about this process to either of the following:

- David Porter, EPD, by either of the following:
 - e-mail to **david.porter@wdc.usda.gov**
 - telephone at 202-720-9865
- HSPD-12 Help Desk by either of the following:
 - e-mail to **USDAHSPD12Help@dm.usda.gov**
 - telephone at 888-212-9309.

Reminder E-Mail with Rekeying Instructions

The following is an example of the instructions received with the reminder e-mail.

Subject: USAccess - ACTION REQUIRED: Update Your USAccess Credential (PIV Card)

Our system indicates that the digital certificates loaded on to your USAccess credential must be updated. You must complete this update *by the close of business before Feb XX, 2011* or your credential will be terminated.

IMPORTANT: If you do not complete the update by the date indicated and your credential is terminated, you will have to re-enroll to obtain a new credential. To re-enroll, you must visit a USAccess enrollment center to present your identification documents, submit fingerprints and have your picture taken again. You must then wait for your new credential to be printed, delivered and activated.

During this time, you may not be able to log on to your work computer or gain access to government buildings if you currently use your USAccess credential for these purposes.

To avoid this inconvenience and delay, please follow the steps below for completing the certificate rekey/update process as soon as possible.

How to rekey/update your credential

To rekey the certificates on your credential, please visit an Activation station or USAccess credentialing center. You must bring your current credential with you, and you must know your PIN. You will be prompted by the system to enter in your PIN to complete the rekey process.

If you do not know your PIN, visit the PIN Credential page located on the USAccess Web site at <http://fedidcard.gov/credreset.aspx> for instructions on how to retrieve or reset it.

Once you have your PIN, please proceed with visiting an Activation station near you, or making an appointment at your local USAccess Credentialing Center. Instructions for making appointments at USAccess Centers are located on the USAccess Web site at <http://fedidcard.gov/credappointments.aspx>.

NOTE: The actual process for certificate rekey takes only a few minutes once the credential is inserted into the card reader if you have your PIN ready before you attempt renewal. If you do not know your PIN, you will need assistance from the Center operator which could add extra time to the process.

Questions?

If you have any questions on this process, please contact your USAccess/HSPD-12 Sponsor, your badge office, HSPD-12 help desk or agency HSPD-12 POC.

*** This email was generated by an automatic process. Please do not reply to this email.

If you have any questions or concerns, please contact your supervisor or your Agency's security office.***