Table of Contents

Overview

Introduction

User access to CIPPS data files is controlled through SECURE, the Millennium security system. CIPPS security IDs and passwords are controlled and administered by the DOA Payroll Security Officer based on agency requests. Several different CIPPS security levels (security profiles) are available to accommodate the functional needs of agencies to process, review, and certify CIPPS payroll and leave data. If users attempt to perform functions for which they do not have security access, a '**SECURITY VIOLATION"** message appears on the screen.

Security Levels

Levels of Security

Six security levels are available to CIPPS users. Agency Payroll Security Officers are responsible for requesting appropriate security levels for agency staff and for monitoring security levels to ensure conformity with the requirements of their current duties.

Level	User Profile	Purpose
1. Update Payroll	User can enter payroll transactions and change Employee and Tax Masterfile information for all CIPPS screens listed on the DBID Table in CAPP – Cardinal Topic 50110, *CIPPS Navigation* and the NSSA Table in CAPP – Cardinal Topic 50125, *Programmatic Data*.	Data entry and routine payroll processing.
2. Update Leave	User can enter leave transactions and change all screens required to process leave. See CAPP – Cardinal Section 40000, *Leave Accounting*.	Data entry and routine leave processing.
3. Certification	User can access the certification screen, PYCTF, and display other CIPPS payroll screens. Users must be authorized by Agency Head to approve and release payrolls for payment, as specified on the Authorized Signatories Form (DA-04-121).	Authorize agency payruns resulting in payroll disbursements and supervisory review.
4. Display Payroll	User can display all CIPPS payroll screens.	Supervisory Review
5. Display Leave	User can display all CIPPS-Leave screens.	Supervisory Review
6. Other	User can update or display specific screens, including NSSA for non-payroll users.	Subject to DOA approval.

Security Levels, Continued

Segregation of Duties

Sound internal control over payroll demands a separation of the payroll data entry and certification functions. Individuals with *Certification* access should not request access to *Update Payroll*.

Agency Payroll Security Officer

Agency Payroll Security Officer

Payroll Security Officers are designated on the agency's Authorized Signatories Form (DA-04-121). Individuals identified as Payroll Security Officers have a "PSO" following their name. It is recommended each agency should have at least two Payroll Security Officers to ensure adequate coverage.

Continued on next page

Agency Payroll Security Officer, Continued

Duties of the Agency Payroll Security Officer

The primary function of Agency Payroll Security Officers is to manage the access of agency personnel to payroll systems including CIPPS, Payline/PAT and CIPPS FINDS. The Payroll Security Officer must:

- Ensure that adequate internal controls exist within the agency to prevent unauthorized access to CIPPS, Payline/PAT and CIPPS FINDS.
- Ensure that each logon ID is assigned to an individual, not a group or section.
- Sign Security Authorization Request forms to add, change, or delete user access to each system. CIPPS security levels are discussed later in this topic. Information regarding Payline/PAT and CIPPS FINDS security levels may be found in CAPP Topic Nos. 70515 and 70710, respectively.
- Ensure records are maintained documenting security activity related to each individual (e.g., copies of CIPPS, Payline/PAT or CIPPS FINDS Security Authorization Requests submitted to DOA, report of users provided by DOA which has been reviewed and verified. (It is strongly suggested the report be signed and dated at the time of review).
- Review the semi-annual Payroll Security report distributed by DOA. Complete the necessary security forms for any changes that need to be made within the agency. Sign and return the semi-annual verification report and forms within two weeks of the date received. Failure to comply may result in removal of all security access for that agency.

Note: Access to CIPPS FINDS by individual agencies will be removed when CARS is de-commissioned. Use of the Payroll Audit Tool (PAT) can provide the same download functionality. Refer to CAPP Topic No. 70735, *Payroll Audit Tool (PAT)*. Additionally all CIPPS reports will be continue to be available through Reportline.

Establishing a CIPPS Logon ID

Introduction

The steps required to establish a CIPPS logon ID require involvement by agency personnel who are familiar with both CIPPS processing and agency internal controls. Coordinated action is required between the following units and individuals:

- Agency Payroll and/or Human Resource offices
- Agency CICS (ACF2) Security Officer. To identify your CICS (ACF2) security officer, contact the Virginia Information Technology Agency (VITA).
- Agency Payroll Security Officer
- DOA Payroll Security Officer

Security planning is crucial due to the number of individuals involved. Remember, each user must have a valid CICS (ACF2) logon prior to accessing CIPPS. See the VITA Website for procedures on obtaining a CICS logon ID. Plan to take initial action at least three weeks in advance of the anticipated date system access is required.

CIPPS Security Authorization Request

The CIPPS Security Authorization Request form is located on DOA's website under DOA Forms. A CIPPS Security Authorization Request form must be submitted to the Payroll Security Officer at DOA each time a CIPPS security action is requested. *CIPPS access is only available to employees of the Commonwealth.* The following information is required:

- Signature of agency's Payroll Security Officer.
- Action requested (new, change, delete).
- Type of access (if new or change).
- User information (name, signature, Employee #, phone number).
- ACF2 logon ID.
- Date of request.

When DOA completes the requested action, a signed and dated copy of the CIPPS Security Authorization Request form is returned to the agency along with an updated CIPPS/Payline Current Users report. Both documents should be reviewed, approved and retained in the agency's CIPPS security file. Auditor of Public Accounts (APA) staff will ask to review these security forms during an audit

Continued on next page

Establishing a CIPPS Logon ID, Continued

CIPPS Passwords

CIPPS passwords are assigned by the DOA Payroll Security Officer and consist of three key fields:

Field	Description
TERM/GROUP	Unique to each agency.
OPERATOR	Unique to each user.
PASSWORD	Originally established by DOA.
	Must be changed by user.
	Contains any alphanumeric identifier up to ten characters.
	A non-display CIPPS field to prevent the password from being seen by other users.
	Expires in 30 days.
Payroll Security Officers should emphasize to users the importance of never sharing passwords.	

Changing CIPPS Passwords

Upon initial establishment and every 30 days thereafter (when the message **A522F-PASSWORD EXPIRED** appears), CIPPS users must change their own passwords during Millennium sign-on. A password cannot be changed more than once in the same day and it ***cannot equal any one of four previous passwords.*** See CAPP – Cardinal Topic No. 50110, *CIPPS Navigation*, for guidance on how to access the Millennium sign-on screens. Follow the steps below to change your password:

Step	Action
1	Enter Term/Group ID, press the Tab key
2	Enter Operator ID, press the Tab key
3	Enter current Password, press the Tab key
4	Enter New Password, press the Tab key
5	Enter New Password in the Verify New Password field, press the End key

CIPPS passwords expire after 30 days but may be changed any time prior to expiration. The password should be changed the day after it is established by DOA and whenever a user thinks the password's integrity has been compromised.

Continued on next page

Establishing a CIPPS Logon ID, Continued

Common Problems and Hints

When entering data in the Password, New Password, or Verify New Password fields, the data entry is hidden. Keying errors or lingering keystrokes may exist in the field. Therefore, it may be necessary to "clear to the end" of these fields to remove any residual, unwanted keystrokes. Generally this is achieved by pressing the END/EOF key. If an error message is received while signing on to CIPPS, review the table below to determine a corrective action prior to calling DOA for assistance:

If this Error Message displays…	**Then, the cause of error is…**	**And, to correct the error…**
ACF01013 LOGON ID… SUSPENDED BECAUSE OF PASSWORD VIOLATIONS	Three attempts at signing onto CICS using the wrong password.	Contact the agency's ACF2 Security Officer or the VITA Help Desk: Local (804) 786-3932 or 1-866-637-VITA (3932). **Do not contact DOA**.
1474F-INVALID TERM/OPER/ PASSWORD	Incorrect data entered in one of the three key security fields.	Re-enter the Term/Group, Operator, and Password after verifying their accuracy and pressing the **clear to the end of the field** key.
A520F-NEW PASSWORD EQUALS PREVIOUS	The password entered in the New Password and Verify New Password Fields is one of the four passwords previously used.	Enter a password that has not been previously used. Make sure to press the **clear to the end of the field** key.

Internal Control

Internal Control

Verification of the appropriateness of security actions and levels must be performed by the agency Payroll Security Officer prior to submission of the CIPPS Security Authorization Request form to DOA. Agencies must develop in-house procedures governing the levels of security requested. Additionally, the timely submission of requests to delete access for terminated/transferred employees is imperative to safeguard the assets of the Commonwealth. All copies of CIPPS Security Authorization Requests and Agency Security Reports must be maintained by the agency for audit purposes.

Records Retention

Time Period

Retain *CIPPS Security Authorization Request* forms and *Agency Payroll Security Reports* on file three years following deletion of access. Do not discard any CIPPS Security Authorization forms for employees with active access. The Auditor of Public Accounts will require a complete security history for these individuals.

Contacts

DOA Contact

Director, State Payroll Operations
Voice: (804) 225-2245
E-mail: Payroll @doa.virginia.gov

Payroll Support Analyst/Trainer
Voice: (804) 786-1083
E-mail: Payroll@doa.virginia.gov

Subject Cross References

References

CAPP – Cardinal Topic No. 40000, *Leave Accounting*
CAPP – Cardinal Topic No. 50110, *CIPPS Navigation*
CAPP – Cardinal Topic No. 50125, *Programmatic Data*
CAPP Topic No. 70515, *Payline Requirements*
CAPP Topic No. 70710, *FINDS: CIPPS System Overview*

CARS to Cardinal Transition

Cardinal Transition

CIPPS interfaces to both CARS and Cardinal. No additional action needs to be taken by agencies in order to record CIPPS entries. After CARS has been decommissioned, agencies will no longer use NSSA to establish programmatic data in CIPPS. Instructions on how to load this information to CIPPS will be distributed at a later time.

Access to CIPPS FINDS by individual agencies will be removed when CARS is de-commissioned. Use of the Payroll Audit Tool (PAT) can provide the same download functionality. Refer to CAPP Topic No. 70735, *Payroll Audit Tool (PAT)*. Additionally all CIPPS reports will be continue to be available through Reportline.