



CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

QUALITY ASSURANCE REVIEW FINDINGS REPORT NO.: 2025 QAR-04

PYRL Access Review

The Post Audit Subsection of the Bureau of State Payrolls (BOSP) has completed a Statewide review of FLAIR PYRL User ID's as of March 20th, 2025.

PURPOSE

The objective of this review is to ensure that User IDs were being terminated immediately upon employee separation, that user IDs were not being shared to bypass internal controls, & that they are being used in accordance with recommended Payroll Preparation Manual guidelines & requirements in Volume V, Section 1.

SCOPE

All agencies that have a minimum of one employee with access to the FLAIR/PYRL system, whether they be an Access Control Custodian for the agency, or a production account with payroll processing functions.

BACKGROUND

An on-line system must have security measures to prevent unauthorized persons from accessing computer files. Authorized personnel must be allowed access to only those files for which they have authority. This is achieved through the use of sign-on procedures and carefully controlled maintenance of the Access Control File.

The Access Control File contains the valid organization codes and initials of employees authorized to access the system. This file is checked each time an organization code, initials and password are entered, and access is not allowed if the entered organization code, initials, and password are not included in the file. Also included in the file are the authorized functions for each organization code/initial combination. Access is allowed only to those functions that are included on the file for the entered organization code/initial combination.

There are two types of access: Access Control sign-on and Operating sign-on. The Access Control sign-on grants access only to the Access Control File and the Operating sign-on grants access only to operating files. A single sign-on cannot access both Access Control and Operating files.

Volume 5, Section 1 "Payroll System Access", subsection C (2)(3) "Review of Security Measures" of the Payroll Preparation Manual, states the user ID is made up of 3 alphanumeric characters and should always consist of the user's initials. The "DESCRIPTION" field is reserved for the Employee ID (People First Login ID, not Appointment ID or Position ID) and the employee's position title. This information is required to be entered for all users.

Methodology

The Post Audit Team obtained the list of all User IDs currently active from PYRL which details information such as User Group, Group Level, Org Code, User ID, ACC status, Name and Description. The data was collected for the report, on March 20th, 2025.

- All active PYRL Access Control User ID's (398 IDs) were the sample population for review.
- Each employee's Access Control Custodian status was validated.
- Each employee's job status was reviewed via People First to ensure the employee was currently employed with the agency who established the PYRL access.

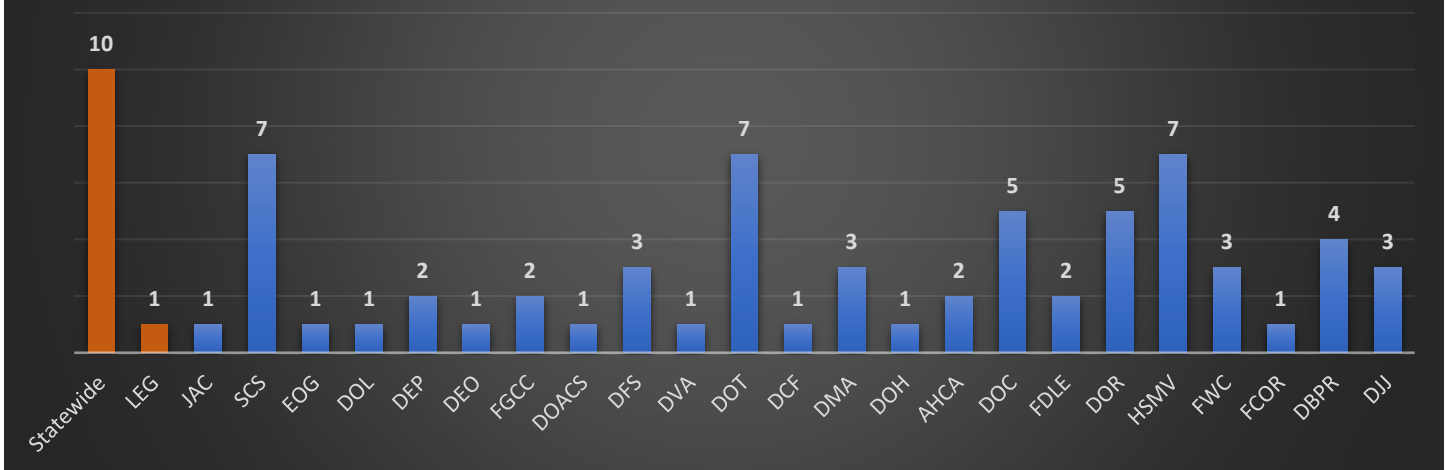
CONCLUSIONS

Out of 34 possible agencies and an additional grouping of Statewide Users, 24 agencies and the statewide group (71.4%) contained a total of 75 findings from reviewing 398 PYRL IDs (18.8%). These findings can be placed into one of the following categories:

1. (42) Fails to meet PYRL description requirements per PPM - Incorrect Employee ID.
2. (28) Fails to meet PYRL description requirements per PPM - No Employee ID provided
3. (1) Separated Employee w/Active PYRL Access
4. (4) Multiple or shared accounts.

Seventy of the 75 findings (**93.3%**) were not in compliance with **Volume 5, Section 1** of the **Payroll Manual**. The remaining five of the 75 findings (**6.6%**) are attributed to PYRL Users with active access that were either not currently employed with that agency or have a second active account at the time of the review.

All Findings: Failure to meet PYRL Description Requirements, per Volume 5, Section 1 of the Payroll Preparation Manual



In the 86 working days of January through the end of April 2025, there were 118 user access additions, 23 of which provided no employee ID in the add process (19.5%). There were 35 user access deletions, of which 7 provided no employee ID upon deletion (20%), and 105 user access edits were completed, and the Agency ACC did not provide an employee ID for 14 of those edits (13.3%). In total, there was a total of 258 PYRL Access transactions, and during each process of adding, deleting, or editing access an employee ID was not provided 17.1% of the time (44 transactions). This process is continuous, and agencies should strive at completing these transactions with the highest of accuracy to remain complaint with the PPM's provided guidance.

Fails to meet PYRL description requirements per PPM - Incorrect Employee ID

Agencies either mistakenly used an appointment ID, entered an incorrect People First ID in error, or did not provide a position title as required in **Volume 5, Section 1** of the *Payroll Preparation Manual*. Forty-two of the 75 agency findings **(56%)** are attributed to this “**Incorrect Employee ID**” grouping.

- Five of the 42 accounts showed an incorrect People First ID in error. **(11.9%)**
- Eight of the 42 accounts incorrectly list a Position ID. **(19%)**
- 26 of the 42 accounts incorrectly list an Appointment ID. **(61.9%)**
- Three of the 42 accounts incorrectly list an Appointment ID and had no position title. **(7.1%)**

Fails to meet PYRL description requirements per PPM - No Employee ID provided

Agencies either did not provide a People First ID or did not provide a position title as required in **Volume 5, Section 1** of the *Payroll Preparation Manual*. Twenty Eight of the 75 agency findings **(37.3%)** are attributed to this “**No Employee ID provided**” grouping.

- 23 of the 30 accounts provide no People First ID. **(76.7%)**
- Five of the 30 accounts provide no People First ID and no position ID. **(16.7%)**

Separated Employee w/Active PYRL Access

A Department of Corrections employee’s access was not removed upon the completion of the employee’s last day of employment, March 4th, 2025. The separated employee’s access was systematically purged on April 11th, 2025, nearly 6 weeks after separation.

Separated Employees w/Active PYRL Access	
Dept. of Corrections	1

Multiple or shared accounts.

Four of the 75 agency findings **(5.3%)** are attributed to this grouping. Two employees appear to have had a second access within the same agency.

Users w/PYRL Access that Cannot be Validated (6)

There were six user IDs identified that could not be validated via People First and/or PYRL. They are listed with DMS as “Problem Resolution Specialist” in their descriptions. DMS/People First has confirmed that they are contractors with Alight/NGA (Northgate Arinso) Human Resources. They support the Refunds and Reconciliation teams in Operations within the People First Service Center.

AGENCY RESPONSES

Each agency with a finding was sent a notification email of findings and was asked to review all their current users with PYRL access and make the necessary adjustments to adhere to the requirement shown in Volume V, Section 1(C) of the Payroll Preparation Manual, as well as agencies with separated employees and the timely removal of access upon separation.

All 24 agencies that were notified of their findings acknowledged the findings, replied with assurances that the findings were corrected or would be corrected, or that a process was put in place to ensure the correct information is used when creating or updating PYRL Access profiles.

RECOMMENDATIONS

BOSP Post Audit made recommendations to three of the agencies that they establish back-up ACCs who can share responsibilities for the primary ACC; including, but not limited to, resetting passwords, reinstating access, updating, or adding accesses without requiring permission from the supervisor.

Department of Environmental Protection (DEP), Florida Commission on Offender Review (FCOR), and Florida Gaming Control Commission (FGCC) do not have back-up ACC's.. For the 3rd consecutive year, FGCC's ACC had been revoked from the system at the time of this report, which is conducted annually. Two agencies did not respond to our request to establish a back-up ACC, and one did establish a back-up ACC after BOSP's recommendation.

Separated Employees w/Active PYRL Access

Volume 5, Section 1 "Payroll System Access", subsection A states that the agency Access Control Custodian is responsible for:

- Removing access for employees who should no longer have access to the payroll system due to termination, suspension, or reassignment of duties.
- Monitoring agency user access on a regular basis. It is recommended by BOSP that agencies perform a quarterly review of all users within the agency.

Agencies should ensure that Job changes and terminations be immediately managed by removing affected employees' access using the access control function. There is no rule preventing an agency from removing an outgoing employee's access prior to the last day employed, that decision can be made based on the agency's business needs, however the employee's access should be removed no later than close of business on the employee's last day in their position.

Fails to meet PYRL description requirements per the Payroll Preparation Manual

Volume 5, Section 1 "Payroll System Access", subsection C (2)(3) "*Review of Security Measures*" of the Payroll Preparation Manual, states the following:

- The "**User ID**" is made up of 3 alphanumeric characters and should always consist of the user's initials.
- The "**DESCRIPTION**" field is reserved for the Employee Id (People First Login ID, not Appointment ID or Position ID) and the employee's position title.

Agencies should complete all updates and maintain these practices on a consistent basis, throughout the state (if the agency is not centralized) in the future to assist with the auditing of system accesses and employment verifications.

Establishment of a back-up ACC

Volume 5, Section 1 "Payroll System Access", subsection A states the following: An agency back-up Access Control Custodian should be established for the primary Access Control Custodian. BOSP highly recommends the establishment of a back-up ACC to ensure duties can still be conducted when the primary ACC is out of office or otherwise unavailable.

After review, many of the agencies have not established back-up ACCs or these accesses have purged, which may be problematic if the primary ACC is out for any period. BOSP was required to update the description fields on behalf of these agencies to adhere to the requirements listed in the Payroll Manual for PYRL system access (Vol. 5, Sec. 1).