QUALITY ASSURANCE REVIEW FINDINGS REPORT NO.: 2023 QAR-02

Review of Agency level PYRL User ID's

The Post Audit Subsection of the Bureau of State Payrolls (BOSP) has completed a Statewide review of FLAIR PYRL User ID's as of February 1st, 2023.

PURPOSE

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

SCOPE

All agencies statewide that have a minimum of one employee with access to the FLAIR/PYRL system, whether that be as 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 on the file. Also included on 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.

Methodology

The Post Audit Team obtained the list of all User ID's 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 January 31st, 2023.

- All active PYRL Access Control User ID's (405 ID's) were the sample population for review.
- Each User ID was verified to have been established with the employee's initials, or with an appropriate variation.
- 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. If not employed with that agency, their separation date was recorded, as well as the number of days since they left the agency (as of 1/31/23).

CONCLUSIONS

A summary of findings below were encountered during the review. Out of 34 possible agencies and an additional grouping of Statewide Users, 23 agencies contained 58 findings, which can be placed into one of the following categories:

1. Fails to meet PYRL description requirements per the Payroll Preparation Manual (Vol 5, Sec 1)
2. Separated Employees w/Active PYRL Access

This review did not identify any users with multiple accounts or agencies with shared or generic accounts, although 2 accesses remained active after employee 1 separated, and now there is a new employee using the same id as the separated employee.

- At least one finding was discovered in 23 of 34 state agencies. **(67.6%)**
- There were 58 findings across 405 PYRL ID's. **(14.3%)**
- 53 of the 58 findings **(91.3%)** do not meet PYRL description requirements described in the Payroll Preparation Manual.
- Four of the 58 findings **(6.9%)** are attributed to PYRL Users with active access that were not currently employed with that State Agency at the time of the review. Two of these positions with those agencies now have active employees in those positions.
- In the 65 working days of January, February, and March of 2023, there were 42 more user access additions (22), deletions (1), or user access edits (19) completed where the Agency Custodian did not provide an employee ID.

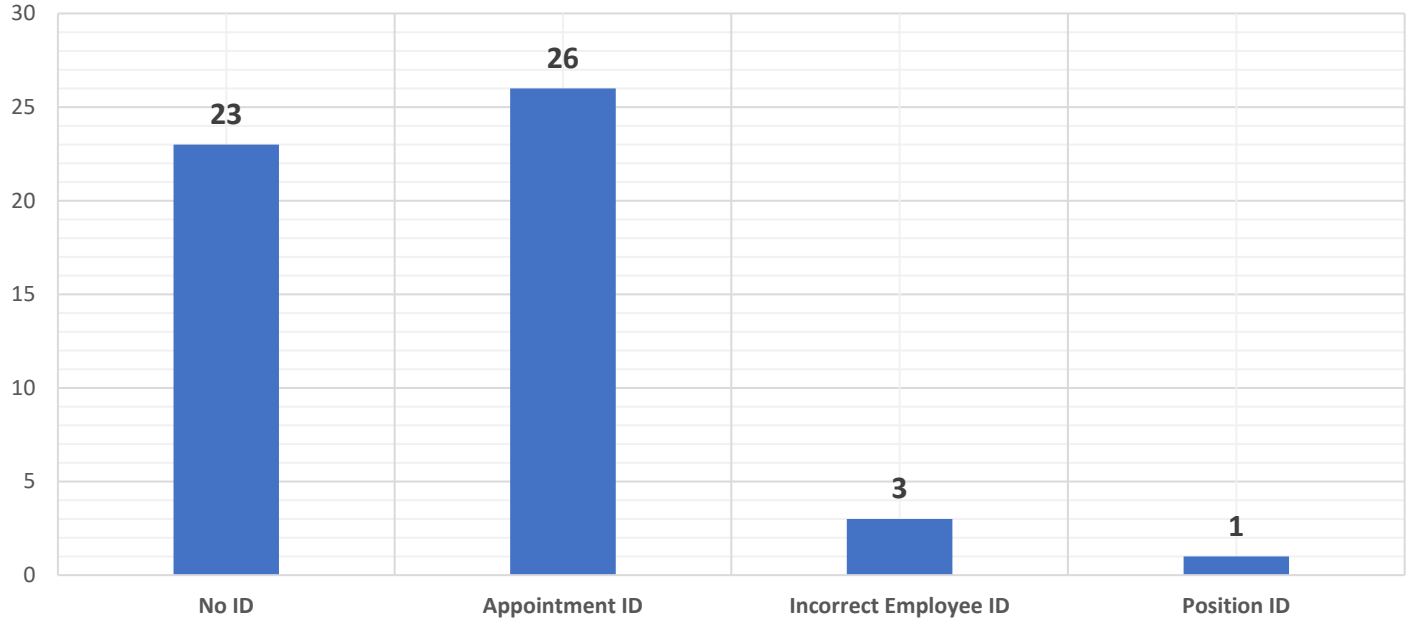
Does not meet PYRL description requirements per the Payroll Preparation Manual (Vol 5, Sec 1)

Agencies either did not provide an employee ID, mistakenly used an appointment ID or position ID, or just entered an incorrect employee ID. 53 of the 58 agency findings are attributed to this category.

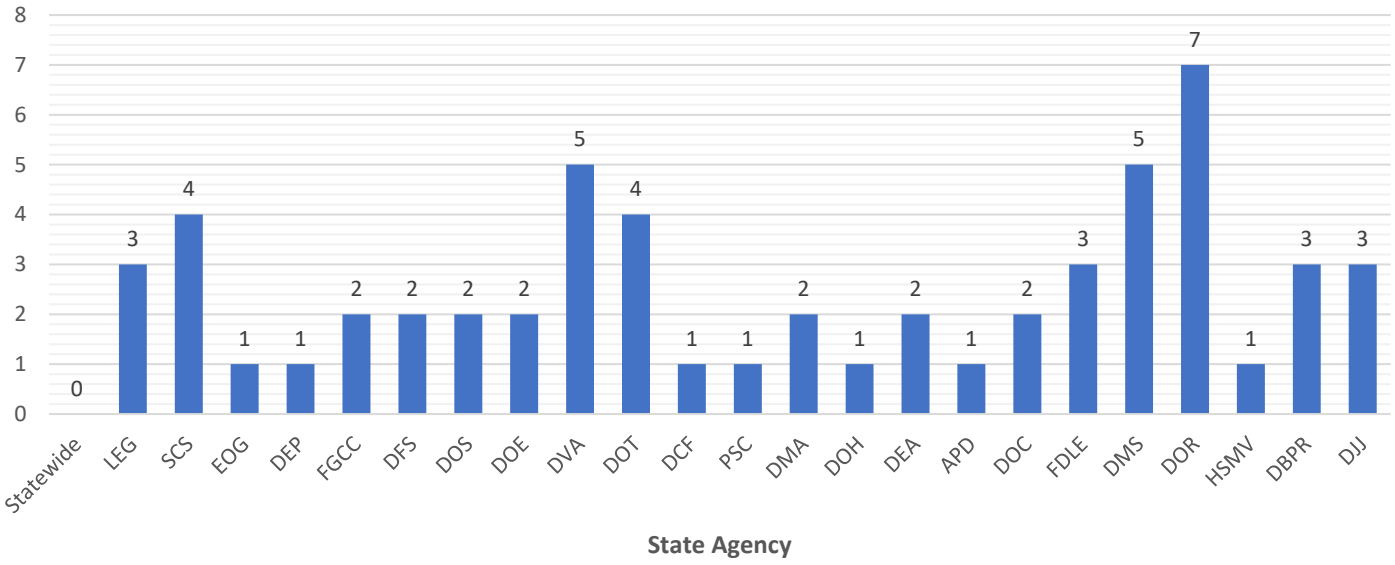
- 23 of the 53 accounts provide no Employee ID. **(43.4%)**
- 25 of the 53 accounts incorrectly list an Appointment ID. (**47.1%**)
- Two of the 53 accounts incorrectly listed a Position ID. (**3.8%**)
- Three of the remaining accounts show an Incorrect Employee ID. (**5.7%**)

The Statewide user group contained 8 user accounts that are assigned to DFS' Office of information Technology (OIT) personnel and therefore restricted and cannot be updated by BOSP, therefore were not included in the findings.

Fails to meet PYRL description requirements per the Payroll Preparation Manual



Agency Findings: Failure to meet PYRL Description Requirements, per the Payroll Preparation Manual



Separated Employees w/Active PYRL Access (3)

Of the PYRL accesses reviewed, three employees no longer worked with the agency that created their access.

A Department of Transportation employee's access was not shut down on the last day of employment, December 26th, 2022, and was systematically purged. This employee later returned to DOT effective 3/13/23, and a new access was established 4/20/23.

Access for an employee with the Agency for Persons w/Disabilities was not shut down on the last day of employment, December 31st, 2022, and remained active as the job position was filled with a new employee.

A Department of Corrections employee moved to another state agency as of January 5th, 2023, and DOC did not remove the access. This access was systematically purged, 2/10/2023.

Separated Employees w/Active PYRL Access	
Dept. of Transportation	1
Agency for Persons w/Disabilities	1
Dept. of Corrections	1

Users w/PYRL Access that Cannot be Validated (2)

There were two 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 description. I received confirmation from DMS/People First 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 of 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.

Twelve of the 23 agencies that were notified of findings, acknowledged the findings, and replied with assurances that the findings were corrected, or that a process was put in place to better assist with the removal of a separated user's access.

Seven of the remaining 11 agencies did not acknowledge the email and findings but did update their users accounts to adhere to the requirements per the Active Access Control (BP89) RDS report provided on July 14th, 2023.

The remaining 4 agencies with a finding did not acknowledge the email or findings, and remain out of compliance, include the Legislature, Department of State**,** Department of Military Affairs, and Department of Business & Professional Regulation**.**

RECOMMENDATIONS

Fails to meet PYRL description requirements per the Payroll Preparation Manual

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

Separated Employees w/Active PYRL Access

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.