DELAWARE RIVER PORT AUTHORITY
STEWARDSHIP. SERVICE. COMMUNITY.

One Port Center
PO Box 1949
2 Riverside Drive
Camden, NJ 08101

(856) 968-2000
(856) 968-2001 Fax
www.drpa.org

David J. Aubrey, CIA, CFE
Inspector General
Office of the Inspector General

OIG Memorandum

TO: K. A. LaMarca, Director, Information Services

FROM: D. J. Aubrey, Inspector General

SUBJECT: Audit of SAP User Access Management Process

DATE: November 7, 2018

The Office of the Inspector General (OIG) has recently completed an audit of Information Services' (IS) SAP User Access Management process. This review was performed by Ron McReynolds, IT Auditor.

A. Objective / Scope

The objective of this audit was to determine that only authorized and active users have access to the Authority's SAP system and the associated data, and that an established and effective process is in place to ensure this control objective is achieved. To achieve our audit objectives, the limited and focused scope included:

- comparing the current SAP user list to an independent list of current DRPA / PATCO employees as of July 30, 2018;
- documenting and communicating any differences determined from the file comparison to Information Services' management for explanation and/or resolution; and,
- identifying any observed gaps in the SAP user access management process (additions, changes, terminations / expirations) and providing recommendations for process improvement (if needed).

OIG compared a current list of active SAP users to a current list of active employees (as of July 30, 2018) provided by Human Resources Services. The two lists were analyzed for non-matching users, and the non-matching users list was provided to Information Services' management for their analysis and feedback. In addition, OIG reviewed Information Services' Policy #510, Access Control Policy and Policy #512, IS Audit Policy for adherence, effectiveness, and any identifiable opportunities for improvement.

B. Analysis

Based on OIG's review, the following points contributed to the conclusions regarding Information Services' SAP User Access Management process:

- the current list of active SAP user accounts had 247 accounts that did not match the current list of active employees (based on comparison of active and current Authority email addresses) provided by Human Resources Services;
- 69 former Authority employees had active user accounts in SAP (30% of the 247 accounts identified);
- 6 former consultants / contractors had active user accounts in SAP (2% of the 247 accounts identified);
- 10 IS "Tablet test accounts", used for training during the SAP system pre-implementation period in 2015, were still active in SAP (4% of the 247 accounts identified);
- 4 test accounts in the system's production environment were still active in SAP (2% of the 247 accounts identified);
- 4 accounts associated with current employees that changed their names (marital status) were still active in SAP after a new account was added for them reflecting the name change (2% of the 247 accounts identified);
- 14 dialog type (standard user) accounts were changed to system accounts (6% of the 247 accounts identified); and,
- the remaining 140 accounts identified for review were associated with current employees with non-matching email accounts, had valid system accounts, valid service accounts, valid reference accounts or valid consultant / contractor accounts; these were valid accounts, but some level of user account maintenance / update was necessary (56% of the 247 accounts identified).

C. Conclusions

Information Services' Policy #510, Access Control Policy is not being effectively applied by Information Services. The policy does not define Authority management's (i.e. Chiefs, Directors, Managers, Supervisors, Human Resource Services) responsibility to notify Information Services when employees have been terminated or changed position. This is supported by the fact that 69 former employees still had active user accounts within SAP.

Information Services' Policy #510, Access Control Policy does not provide for effective contractor / consultant user access management. The policy does not define Authority management's (i.e. Chiefs, Directors, Directors, Managers, Supervisors, Human Resource Services) responsibility to notify Information Services when contractor / consultant accounts should be terminated. In addition, the policy does not provide time limits for contract / consultant account access. This is supported by the fact that 6 former contractors / consultants still had active user accounts in SAP with an expiration time limit indicated as the year "9999", or null.

Information Services' Policy #512, IS Audit Policy, mandating quarterly access reviews is not being followed. This is supported by the fact that some of the former employees with current SAP access accounts had left the Authority over 2 years ago and no documented user review has been performed and provided.

The current process for managing SAP User access does not provide consistent user data across the SAP system. This is documented by the fact that 247 SAP user accounts did not have valid employee email addresses assigned to them and several accounts were assigned with incorrect account type (i.e. dialog vs. system). Many more SAP user accounts had to be matched to employees through a first name and last name matching process. Contractors / consultants were not identified in the SAP user account data. The contractors / consultants' accounts did not have any information to associate them with their company and an associated Authority employee / user.

D. Audit Recommendations

As a result of our audit, OIG recommends the following:

Audit Recommendation #1:

Information Services' Policy #510, Access Control Policy should be updated to emphasize Authority management's responsibility to notify the Help Desk by email when employees are terminated or scheduled to be terminated (involuntarily or voluntarily) or change positions within the Authority. Once revised, the policy should be communicated across the Authority to all employees. The Help Desk should retain and categorize all issues related to access changes, additions and expirations in the Solar Winds Help Desk system for 2 years for auditing purposes. The access related issues documentation should be readily available for reporting and review.

Information Services' Policy #510, Access Control Policy should be effectively and consistently applied by the Help Desk across all systems, and not just for network access.

Management Response #1:

Agree. IS will modify the policy but will not be responsible for managing the communication from other departments. Target date: March 31, 2019.

Audit Recommendation #2:
A new Information Services' policy (Contractor / Consultant Access Control Policy) should be written to provide guidance for Authority management regarding system access for all non-Authority employees needing system access. This policy should define Authority management's responsibility to notify the Help Desk when a contractor / consultant's access should be terminated. The policy should restrict contractor / consultant's system access to 3 months with renewal authorization for incremental 3-month periods by the responsible Authority management. The responsible management overseeing the contractor / consultant should have a responsible employee's email address in the user account of the contractor / consultant. Once written, the policy should be communicated to all Authority employees.

Management Response #2:
Agree. IS has a PCI policy that covers access control for consultants. IS will create a new policy that will applicable Authority-wide (both PCI and non-PCI environments). The policy will also incorporate the requirement for consultants to have their laptops scanned and checked for updated anti-virus software. The policy will be applicable for all systems. Target date: March 31, 2019.

Audit Recommendation #3:
Information Services' Policy #512, IS Audit Policy, mandating quarterly access reviews, should be conducted by Information Services across all systems, documented, and available for review.

Management Response #3:
Agree. IS will establish a process and procedure for the Help Desk to perform bi-annual access reviews of all systems. IS will also update Policy #512 to reflect the reviews. Target date for completion of process and procedure: March 31, 2019

Audit Recommendation #4:
Regarding standard user account set-up and maintenance:

a. SAP user accounts should require a valid Authority email address for all employees and should include as much information as possible to identify the employee (i.e. phone number, title, Department, Department location, etc.).
b. All current and future SAP contractor / consultant user accounts should be updated with the current and active Authority email address of the responsible Authority employee that is sponsoring the contractor / consultant, and as much information as possible to identify the contractor / consultant (i.e. firm name, description, phone number, office address, etc.).
c. User groups should be created and updated in SAP to define all user accounts.

d. All SAP user accounts with types (B - System, C - Communication, L - Reference, S - Service) should include the valid email address of the responsible Information Services employee who can verify that the account is valid and still necessary. These types of user accounts should have as much information as possible in SAP to describe the purpose of the accounts in the event the IS employee is no longer associated with the Information Services group (i.e. retired, terminated, promoted, relocated).
e. New SAP accounts should not be created for users that change name (i.e. marital status change) and two active accounts for the same user should not be permitted. Their current account should be modified with as much information as possible, including previous name and date changed. This account administration technique will maintain the audit trail for transactions previously processed.
f. SAP Test accounts should not be created in the SAP production environment. SAP Test accounts should only be created in the test / development environment.
g. The active user accounts currently in the SAP system should all be updated with as much information as possible to reflect the new process for defining users per the new procedure, particularly current and correct email addresses.

Management Response 4:

a. Agree. IS will update the account information for all DRPA employees to reflect the Authority email address as well as other personnel information. Target date: March 31, 2019.
b. Agree. In most cases an SAP user account will not have an associated Authority email address. In those cases, the account will be updated with the email address of the Help Desk. This would be applicable to all systems (not just SAP). Target date: March 31, 2019.
c. IS will explore the possibility in our current system. Update will be provided by March 31, 2019.
d. Agree. IS will update those accounts showing responsibility with the Help Desk as they are creating and auditing the accounts. Target date: March 31, 2019
e. Disagree. System limitations do not allow this recommendation. However, the Help Desk can create a new account and disable the old account. We will add notes in t-code SU01 for the old account and then have the new account be the responsible person for the old account.
f. Agree. There are currently no test accounts in the Production environment.
g. Agree. Prior to the drafting of this memo, IS was provided by OIG a listing of 247 accounts that did not comply with the recommendations as stated above. All of those accounts have been accurately updated.

Audit Recommendation 5:
Help Desk personnel should be trained to determine the correct user account type for the user access requested. Help Desk personnel should be trained to determine the correct user group to be used (a "null" user group should not be allowed; all users should be defined by an existing category, i.e. consultant, employee, system, service, etc.).

Management Response 5:
Agree, however, this will be based on the outcome of Management Response 4c. If creating distinct user groups is possible, the Help Desk will be trained accordingly on the creation of those user groups. We will then move the accounts to the new user groups. Target Date: March 31, 2019.

Improving the SAP user access management process through the implementation of the suggested recommendations will lower the Authority's risk of a system breech by former employees, contractors and consultants. Also, the recommendations will provide an easier process for Information Services when completing quarterly user access reviews in compliance with Information Services' Policy #512, IS Audit Policy.

OIG wishes to thank K. LaMarca, Director, Information Services, for his cooperation and assistance during the completion of this review, as well as T. Brown, Chief Administrative Officer and S. Thompson, Human Resource Services, for their assistance in providing requested information to complete our audit.

cc: R. Boyer
J. Nash
E. DePasquale
R. Taylor
S. Murphy
A. Nelson
J. Hanson
M. Wing
T. Brown
R. McReynolds