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 DRPA Active Directory System

DATE: February 19, 2021

The Office of the Inspector General (OIG) has recently completed an audit of the Authority's Active Directory system. The Active Directory system is managed by Information Services (IS). This audit was performed by Ron McReynolds, IT Auditor.

A. Objective / Scope

The audit's objective was focused on assessing the Authority's Active Directory implementation and management, security design effectiveness, operating effectiveness of the security controls, and identifying any unauthorized users. To accomplish the objectives, the scope of this audit focused on the configuration controls relating to:

- Active Directory management;
- secure Active Directory boundaries;
- secure domain controllers;
- secure domain and domain controller configuration settings; and,
- secure administrative practices.

B. Background

As general background, Windows Active Directory is the underlying technology within the Microsoft Windows' operating system that provides for an integrated and single sign-on system that addresses security, access and identity management. Active Directory allows for a centralized management of users and their security, and provides a central repository that contains user IDs, user permissions, and audit processing. Active Directory is implemented on Domain Controllers, which control the various users and computers within the Domain Controller's scope. The key area to assure an effective and secure Active Directory resides within the configuration settings established during its implementation, and the subsequent maintenance of this configuration during the life cycle of the Active Directory. Failure to effectively design and manage Active Directory controls could result in:

- disruption of computing services;
- destruction of enterprise data;
- disclosure of sensitive information, including identities, intellectual property, etc.;
- reputational risk and loss of confidence by stakeholders, business partners and customers due to disclosure of information or related publicity;
- fines and penalties;
- lost productivity due to inefficient security administration; and,
- security breaches.

C. Analysis

Information Services is currently implementing a migration of users to a new primary domain named "DRPA" from the old primary domain named "WKTRM". This migration is facilitating the upgrade of the Authority's computers to the Microsoft 10 operating system. The migration project is being managed internally.

Based on OIG's review, the following points contributed to the conclusions regarding Information Services' Active Directory process:

- OIG requested from Information Services the topology documentation outlining the structure of the Active Directory domain relationships. This topology is used to optimize speed and efficiency of the network, as well as, provide basic overview to management of the Active Directory structure. Information Services did not have an updated topology but provided a topology from a consultant that outlined the current Active Directory structure versus a soon to be implemented structure for Microsoft 10 operating system. This topology did not detail the organizational relationships of the domains;
- OIG requested from Information Services the implementation and design documentation from the original project to implement the Active Directory system. Information Services did not have any of this documentation;
- OIG requested from Information Services the standard operating procedures governing the Active Directory, the documented policies governing the approval

process for the Active Directory, the documentation detailing the Organizational Unit (OU) groups and their relationship in the Active Directory. Information Services did not have any of this documentation;

- OIG requested direct read-only temporary access to the Active Directory, but Information Services would not provide access. OIG requested a download of all user accounts in a spreadsheet. Information Services provided spreadsheets for enabled users in the primary domains “DRPA” and “WKTRM” and spreadsheets for the disabled users in the primary domains “DRPA” and “WKTRM”. The enabled user spreadsheets were compared against a list of employees from the SAP Human Resources system. The “DRPA” domain had 1,079 enabled user accounts that were non-employees. The “WKTRM” had 654 enabled user accounts that were non-employees. The non-employee accounts were sent to Information Services to be identified. As identified by Information Services, many of these non-employee accounts are elevated privileges accounts, consultant accounts, system accounts, test accounts, separated employee accounts, unidentified user accounts etc. Information Services stated that approval documentation does not exist for these accounts;
- OIG requested from Information Services a screen shot of the password settings and configuration. Information Services provided the screen shot and the settings and configuration were within industry standards;

D. Conclusions

The Authority’s Active Directory system is currently administered and managed in a reactive manner with little to no documentation. Information Services provides access and separation when requested.

There are currently no documented processes or procedures in place to evaluate current users in the Active Directory per Information Services Policy #512 which mandates bi-annual access review. Information Services’ Manager, ERP and Applications, has acknowledged that he has recently taken over responsibility for the Active Directory system and a User Review is needed. Many of the non-employee accounts in the Active Directory system are invalid and should be disabled to prevent improper access to the Authority’s systems. The procedurally required bi-annual review will help to prevent any administrator from creating a back door into the system.

There are currently no documented processes or procedures in place for management oversight of: user access, technical system policy changes, and permission rights for OU groups. The lack of documentation prevents management oversight of changes to the system and does not provide for appropriate knowledge transfer should the IS administrator(s) separate from the Authority.

The Active Directory system has many accounts with elevated privileges. In the event of a breach, these accounts provide excessive risk of full network exposure to unauthorized changes, denial of service attacks, malware attacks and ransom ware attacks. The policy of least privilege access should be followed.

The vendor/ consultant / temporary employee accounts do not have expiration dates. These accounts should have a 3-month expiration date with an opportunity to request renewal of access by the responsible Authority personnel.

E. Audit Recommendations

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

Audit Recommendation #1:

Information Services should complete a thorough user account access review of the Active Directory system and take a proactive approach for system security.

a) All accounts with elevated privileges should be reduced to minimum privilege access except for the Active Directory administrators and the IS manager (ERP and Applications).
b) All current and future contractor / consultant / temporary employee accounts should be updated with the current and active Authority email address of the responsible Authority employee that is sponsoring the contractor / consultant / temporary employee, and include as much information as possible to identify the contractor / consultant / temporary employee (i.e. firm name, description, phone number, office address, etc.). These accounts should have a 3-month expiration date.
c) All former employee accounts should be disabled.
d) All system accounts should be evaluated and the unnecessary accounts disabled including test accounts.
e) Information Services should create formal documented procedures detailing the user account access review process as part of Recommendation #3

Management Response #1:

In reference to item A, IS currently uses the following structure for access levels:
Domain Admin – This is reserved for the Active Directory administrators and IS Manager, ERP & Applications.

- Server Admin – This is reserved for IS staff that need access to servers to perform troubleshoot and/or routine maintenance. Access is granted to staff that is responsible for the respective server.
- Workstation Admin – This is reserved for IS staff to access desktop PC's to perform troubleshooting and/or routine maintenance.
- User account – This is a standard user account that is given to the remaining users.

In this design, an IS administrator can have four separate accounts to perform their duties. This is a best practice method. Also, access to servers is granted on an as needed basis per server. A server admin account does not grant access to all servers. The only people that would have multiple accounts would be IS staff. A part of the separation process would be to disable all their accounts. As an example, here is the naming convention:

- JSmith.da
- JSmith.sa
- JSmith.wa
- JSmith

In reference to Audit Recommendation 1.b, IS management agrees with the OIG recommendation. We are currently in the process of updating the info of all user accounts. The anticipated completion date is 12/31/21 but may be completed sooner.

In reference to Audit Recommendation 1.c, this process is already be in place. Accounts are disabled when IS gets notified by HR that an employee is ending employment.

In reference to Audit Recommendation 1.d, IS management agrees with the OIG recommendation. Anticipated completion date is 12/31/21.

In reference to Audit Recommendation 1.e, IS management agrees with the OIG recommendation. Anticipated completion date is 12/31/21.

IS management is currently in the beginning stages of a full user audit. This will include an audit of every account to ensure it is in use, needed, and given proper access levels. User information will be updated so it is accurate and a standardized naming convention will be implemented for better organization. As a part of this, audit processes will be created so this information is continually reviewed to ensure access is only being granted as needed. The estimated completion date for this is 12/31/21.

Audit Recommendation #2:
Information Services should create a hierarchal permissions chart detailing the permissions for the OU groups. This documentation will provide management with an understanding of the permissions and the OU strategy.

Management Response #2:
IS management has already developed this hierarchy. This was designed as part of the new domain. OU employee hierarchy is now based on org chart. For non-employee accounts we will have the following hierarchy:

> Consultants – OU's will be created for each organization. Consultants will be placed in these OU's which will keep these users in a central location.
>
> Service accounts – OU's will be created for service accounts grouped by their purpose. They will be easily identifiable when a standardized naming convention is fully in place.

Special purpose – OU's will be created for special purpose as needed. An example would be software that uses unique groups for granting access. These will also be organized by purpose. Generally, these OU's will not gain any additional access within AD but will primarily be used to grant access to other applications such as Public Safety and other systems leveraging AD authentication.

This documentation will be provided once all objects are moved to the new domain. Estimated completion is 12/31/21 but may be completed sooner.

Audit Recommendation #3:

Information Services should create standard operating procedures documentation for the IS administrators of the Active Directory system including a documented change management procedure for system changes and non-employee user account administration. This documentation should include a process for providing an electronic audit trail for these changes (i.e. excel spreadsheet saved to a network drive). This documentation will aid in the knowledge transfer process and management oversight.

Management Response #3:

IS management agrees with the OIG's recommendation and will be completed by 12/31/21.

Audit Recommendation #4:

Information Services should create an Active Directory topology outlining the primary domain (DRPA) and the relationship between the secondary domains and applications using Active Directory data. This document should be reviewed annually and modified when changes are made. This document can be used to optimize the performance of the system. provide better knowledge transfer for new IS staff and keep IS management up to date about changes to the system.

Management Response #4:

IS management does not feel this is necessary as the old domain (WKTRM) will be retired as soon as all objects are migrated to DRPA. About 95% of PC's have been moved and the process has begun to migrate servers. The anticipated completion date is 12/31/21. Once complete, there will only be one domain and a multi-domain environment will cease to exist.

Improving the Active Directory system management process through the implementation of the suggested recommendations will lower the Authority's risk of a system breach by former employees, contractors and consultants, improve the optimization of network resources, and improve management overview. Also, the recommendations will provide an easier process for Information Services when completing bi-annual 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 L. Pavlik, Manager ERP and Applications, Information Services, for his assistance in providing requested information to complete our audit.

cc: C. Parker
J. Nash
T. DeFoor
C. Pike-Nase
A. Nelson
J. Hanson
M. Wing
L.Pavlik
R. McReynolds