



OIG

Office of Inspector General

U.S. Department of State • Broadcasting Board of Governors

AUD-IT-16-37

Office of Audits

June 2016

(U) Management Assistance Report: Inactive Accounts Within the Department of State's Active Directory

MANAGEMENT ASSISTANCE REPORT

~~**IMPORTANT NOTICE:** This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies of organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

(U) Summary of Review

(U) The Department of State (Department) uses a Microsoft for Windows directory service known as Active Directory (AD) to centrally manage network users, groups, and system information, while enforcing security standards and standardizing network configuration. AD allows assignment of access controls to individuals and services based on their respective roles.

(U) Acting on behalf of the Office of Inspector General (OIG), Office of Audits, Williams, Adley & Company-DC, LLP (Williams Adley), an independent public accounting firm, evaluated whether the Department disabled inactive AD user accounts in accordance with its internal policies. According to the National Institute of Standards and Technology, inactive accounts should be automatically disabled after a defined period of time. The Department's AD account policy states that Department officials should disable inactive user accounts after 90 or more days. AD accounts tested for this audit were generated on January 6, 2016 (see Appendix A for details regarding the scope and methodology).

~~(SBU)~~ Of the 40,794 domestic AD accounts tested for this audit, Williams Adley found 2,601 (6.4 percent) had not been disabled after 90 days of inactivity. Of the 2,601 inactive accounts, 1,932 (74 percent) accounts were inactive for more than 1 year, and the remaining 669 accounts were inactive for greater than 90 days, but less than or equal to 365 days. This occurred, in part, because the Department does not have a centralized process for AD account management. According to a Bureau of Information Resource Management (IRM) official, AD account management remains a delegated model in which IRM relies on system administrators within bureaus to manually disable inactive accounts rather than using an automated process to identify and disable inactive accounts as required by the Foreign Affairs Handbook.

~~(SBU)~~ If an unneeded account remains active, an intruder could potentially gain access to the account, elevate and/or change its access permissions, and gain access to sensitive information that could compromise the integrity of the Department's network and cause widespread damage across the Department's IT infrastructure. Moreover, if an intruder gains access to an inactive account with elevated or administrative privileges, the intruder could access personally identifiable information without being detected, creating the risks of data loss and theft and of compromising users' identities and the accountability of users' actions.

(U) In its April 25, 2016, response (see Appendix B) to a draft of this report, IRM did not concur with the two recommendations offered. OIG considers both recommendations unresolved. IRM's response and OIG's reply are presented in the body of this report following each recommendation.

(U) OBJECTIVE

(U) The objective of this audit was to determine whether the Department disabled inactive domestic AD accounts after 90 days, as required by its internal policies.

(U) BACKGROUND

(U) The Department depends on information systems and electronic data to carry out essential mission-related functions. The security of these systems and networks is vital to ensuring the continued operations of the Department. These information systems are subject to serious threats. The overall purpose of identity and access management in an IT system is to ensure that users and devices are authorized to access information and information systems. Users and devices must be authenticated to ensure that they have accurately identified themselves before they obtain access rights. Strong information system authentication requires multiple factors.

(U) One tool used by the Department for identity and access management is AD. AD is a directory service created by Microsoft for Windows domain networks. AD provides the means to centrally manage network users, groups, workstations/computers, servers, printers, network shares, and system information, while enforcing security standards and standardizing network configuration. The Department, which has used AD since 2001, can use this tool to manage network users and groups through user and non-user accounts. Some examples of non-user accounts include mailbox and service accounts. A mailbox is tied to an AD user account or accounts, and the user or users can use the mailbox account to send and receive messages; and to store messages, appointments, tasks, notes, and documents. A service account is a non-user account used to run particular services on applications and servers. AD allows assignment of access controls to individuals and services based on their respective roles.

(U) Microsoft Best Practices¹ explains that AD's Domain Services function assists IT administrators in managing network resources. Through another service, called Rights Management, organizations use AD to safeguard digital information from unauthorized use by allowing IT administrators to define who in the organization can open, modify, or take other actions related to the information. According to Microsoft, once a user account has received authentication and can potentially access an object, the type of access granted is determined by either the user rights that are assigned to the group (or user) or the access control permissions that are attached to the object.

¹ (U) TechNet, <<https://technet.microsoft.com/en-us/library/hh831484.aspx>>, accessed on January 28, 2016.

(U) RESULTS

~~(SBU)~~ According to the National Institute of Standards and Technology,² inactive accounts should be automatically disabled after a defined period of time. The Foreign Affairs Handbook³ states that Department officials must disable inactive accounts after 90 days. Williams Adley determined that the Department was not disabling inactive domestic AD accounts after 90 days in accordance with the Department's internal policy. Specifically, Williams Adley found that 2,601 (6.4 percent) of 40,794 domestic accounts were inactive for more than 90 days and had not been disabled in AD. Of the 2,601 inactive accounts, 1,932 (74 percent) accounts were inactive for more than 1 year, and the remaining 669 accounts were inactive for greater than 90 days, but less than or equal to 365 days.

~~(SBU)~~ OIG reported a similar deficiency in its FY 2015 Federal Information Security Management Act audit report.⁴ Specifically, system owners did not disable 9,321 (7 percent) of 129,201 AD accounts after 90 days of inactivity. Of the 9,321 inactive accounts, 5,378 (58 percent) accounts were inactive for more than 1 year, and the remaining 3,943 accounts were inactive for greater than 90 days, but less than or equal to 365 days.

~~(SBU)~~ In its 2014 report on AD,⁵ OIG stated that the deficiencies it identified with AD Rights Management primarily occurred because IRM had not established a governance structure or strategy to ensure that AD Rights Management was implemented and managed consistently. In addition, OIG reported that AD Rights Management was decentralized, and the Information Management Officers at each bureau or post were allowed to make decisions about implementing and overseeing AD accounts. In its report, OIG included two recommendations,⁶ both of which remained open as of March 2016, that relate to managing unneeded accounts. Specifically, OIG recommended that IRM, in coordination with the Bureaus of Human Resources and Diplomatic Security,

- ~~(SBU)~~ develop and implement an overall strategy that will provide policies and procedures for managing Active Directory account management that reflects the interaction among all bureaus; and

² (U) National Institute of Standards and Technology Special Publication 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

³ (U) 12 FAH-10 H-100, "Unclassified/SBU Information System Security Technical Controls," September 2014.

⁴ (U) OIG, *Audit of the Department of State Information Security Program* (AUD-IT-16-16, November 2015).

⁵ (U) OIG, *Audit of the Department of State Implementation and Oversight of Active Directory* (AUD-IT-15-05, October 2014).

⁶ (U) Recommendations 1 and 3 of AUD-IT-15-05.

- ~~(SBU)~~ develop and implement guidance that describes a sustainable and repeatable process for determining how to identify and then disable or remove unneeded OpenNet⁷ accounts.

~~(SBU)~~ During this engagement, Williams Adley determined that the Department has not taken action to address the deficiencies OIG identified in its 2014 report. Specifically, Williams Adley found that the Department still does not have a centralized process for AD account management. According to an IRM official, AD account management remains a delegated model, where IRM relies on system administrators within bureaus to manually disable inactive accounts rather than using an automated process to identify and disable inactive accounts as stated in the Foreign Affairs Handbook.⁸ Because OIG has open recommendations related to addressing this deficiency, Williams Adley is not repeating those recommendations in this report.

~~(SBU)~~ The Department responded to these findings by discussing its efforts with respect to implementation of personal identity verification⁹ (PIV) cards. According to IRM officials, the Department's goal is to mitigate the risk of inactive AD accounts by using such cards. The Department developed the "Program Management Plan for PIV Login to OpenNet Deployment."¹⁰ In this plan, IRM details the Department's efforts to comply with Homeland Security Presidential Directive 12.¹¹ The first step in doing so was to leverage the use of the PIV cards for domestic bureaus to gain access to OpenNet using two-factor authentication.¹² In January 2016, Williams Adley confirmed this step was completed.

~~(SBU)~~ In addition to using the PIV cards for two-factor authentication, the Department also plans to use the PIV cards for a number of different Department-wide access controls¹³ within 3 years,¹⁴ including granting access to specific applications based on agreed-upon permissions. For example,

⁷ (U) According to 5 FAM 870, "Networks," September 2014, OpenNet is the Sensitive but Unclassified network in the Department, and it provides access to standard desktop applications such as word processing and email.

⁸ (U) 12 FAH-10 H-112.1-1f, "Unclassified/SBU Information System Security Technical Controls," *Account Management*, September 2014.

⁹ (U) According to TechTarget, a personal identity verification card is a U.S. Federal smart card that contains the necessary data for the cardholder to be granted physical and logical access to Federal facilities and information systems, and assures appropriate levels of security for all applicable Federal applications, <<http://whatis.techtarget.com/definition/personal-identity-verification-PIV-card>>, accessed on February 24, 2016.

¹⁰ (U) IRM, "Program Management Plan for PIV Login to OpenNet Deployment," March 2015.

¹¹ (U) Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004, requires mandatory, Government-wide standards for secure and reliable forms of identification issued by the Federal Government to its employees and Federal contractors.

¹² (U) Two-factor authentication requires at least two factors to securely authenticate a user, such as something the user has, something the user knows, and/or something the user "is."

¹³ (U) The Program Management Plan includes the Department's PIV plan for its remote access solution (Global OpenNet), mobile devices, overseas posts, and system administrators.

¹⁴ (U) Cable 15 STATE 113404 "Global Badging and Secure Network Access," September 29, 2015.

if a user has access to a specific application, the PIV card could automatically authenticate and authorize the user to access the application.

~~(SBU)~~ Although the Department has implemented two-factor authentication across all domestic workstations and is working towards the complete implementation of PIV over the next 3 years, its "Program Management Plan for PIV Login to OpenNet Deployment"¹⁵ does not prescribe a method for identifying and removing inactive accounts that are not required to complete the PIV process, such as mailbox, service, and terminated user accounts. The Department's plan will only mitigate the risk of inactive accounts where a user is required to have a PIV card to access the Department's OpenNet; in other words, the plan will only be effective for user accounts.

~~(SBU)~~ If an unneeded account remains active, an intruder could potentially gain access to the account, elevate and/or change its access permissions, and gain access to sensitive information that could compromise the integrity of the Department's network and cause widespread damage across the Department's IT infrastructure. Moreover, if an intruder gains access to an inactive account with elevated or administrative privileges, the intruder could access personally identifiable information (PII) without being detected.

(U) CONCLUSION

~~(SBU)~~ The Department did not comply with its own timeliness requirement for disabling inactive AD accounts, as defined in its internal policies. Specifically, Williams Adley found that of the 40,794 domestic AD accounts tested for this audit, 2,601 (6.4 percent) had not been disabled after 90 days of inactivity. Of the 2,601 inactive accounts, 1,932 (74 percent) accounts were inactive for more than 1 year. Without effective AD management, the risk of unauthorized access is significantly increased and may result in the submission of false transactions, improper access to and dissemination of confidential data, and other malicious activities that may impede the Department's ability to achieve its core mission.

(U) In addition to the open recommendations OIG is tracking from its previous reports regarding identity and access management, OIG is making two recommendations:

Recommendation 1: ~~(SBU)~~ OIG recommends that the Bureau of Information Resource Management develop a plan to effectively identify and remove inactive mailbox, service, and terminated user accounts.

~~(SBU)~~ **Management Response:** IRM did not concur with the initial recommendation, stating that "the Program Management Plan for PIV Login was created to deploy and implement PIV domestically and overseas. Now that IRM has completed that goal, the plan has been completed and does not lend itself to amendment." IRM also stated that it began "an effort to focus its attention on privileged users, including reducing the number of privileged users,

¹⁵ (U) IRM, "Program Management Plan for PIV Login to OpenNet Deployment," March 2015.

improving the process whereby these users get accounts, and tightening the management of application specific privileged accounts." In addition, IRM stated that it "continues to routinely delete stale accounts, and that its Information Assurance Directorate continues to conduct a monthly scrub of inactive accounts."

~~(SBU)~~ **OIG Reply:** OIG considers this recommendation unresolved and has modified the recommendation to clarify its intent. Although OIG acknowledges that IRM developed and executed a plan to implement PIV both domestically and overseas, IRM still needs to develop an effective plan to identify and remove inactive mailbox, service, and terminated user accounts. As noted in this report, of the 2,601 inactive AD accounts identified during this audit, 1,932 (74 percent) were found to be inactive for more than 1 year. OIG therefore concludes that the process IRM is using to identify and remove inactive AD accounts is ineffective.

(U) This recommendation will be resolved when IRM provides a plan of action to implement this recommendation or provides an acceptable alternative to identify and remove inactive AD accounts. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has implemented a process to identify and remove inactive mailbox, service, and terminated user accounts.

Recommendation 2: ~~(SBU)~~ OIG recommends that the Bureau of Information Resource Management implement the plan developed in response to Recommendation 1 to guide the identification and timely removal of inactive mailbox, service, and terminated user accounts.

~~(SBU)~~ **Management Response:** IRM did not concur with the initial recommendation, stating that "the Program Management Plan for PIV Login was created to deploy and implement PIV domestically and overseas. Now that IRM has completed that goal, the plan has been completed and does not lend itself to amendment." IRM also stated that it began "an effort to focus its attention on privileged users, including reducing the number of privileged users, improving the process whereby these users get accounts, and tightening the management of application specific privileged accounts." In addition, IRM stated that it "continues to routinely delete stale accounts, and that its Information Assurance Directorate continues to conduct a monthly scrub of inactive accounts."

~~(SBU)~~ **OIG Reply:** OIG considers this recommendation unresolved and has modified the recommendation to clarify its intent. This audit found that 74 percent of the inactive AD accounts identified had been inactive for more than 1 year, which does not align with IRM's response that it "continues to routinely delete stale accounts, and that its Information Assurance Directorate continues to conduct a monthly scrub of inactive accounts." Without effective AD management, the risk of unauthorized access is significantly increased and may result in the submission of false transactions, improper access to and dissemination of confidential data, and other malicious activities that could impede the Department's ability to achieve its core mission.

(U) This recommendation will be resolved when IRM provides a plan of action to implement this recommendation or provides an acceptable alternative to guide the identification and timely removal of inactive AD accounts. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has developed and disseminated guidance that fosters the identification and removal of inactive mailbox, service, and terminated user accounts.

(U) RECOMMENDATIONS

Recommendation 1: (~~SBU~~) OIG recommends that the Bureau of Information Resource Management develop a plan to effectively identify and remove inactive mailbox, service, and terminated user accounts.

Recommendation 2: (~~SBU~~) OIG recommends that the Bureau of Information Resource Management implement the plan developed in response to Recommendation 1 to guide the identification and timely removal of inactive mailbox, service, and terminated user accounts.

(U) APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY

(U) The Chief Information Officer's corrective action plan¹⁶ that was intended to address prior year OIG recommendations stated that the Department of State (Department) planned to deploy personal identity verification card login to domestic OpenNet workstations by December 31, 2015. In order to track the Department's progress regarding domestic personal identity verification card login implementation, Williams, Adley & Company-DC, LLP (Williams Adley) excluded foreign domains from this engagement.

~~(SBU)~~ The Bureau of Information Resource Management provided the Department's Active Directory listing for January 6, 2016, which contained 14 domains, as shown in Table A.1. According to a Bureau of Information Resource Management official, 5 of those 14 domains are foreign: af.state.sbu, eap.state.sbu, eur.state.sbu, neasa.state.sbu, and wha.state.sbu.

~~(SBU)~~ Once Williams Adley filtered the Active Directory list to reflect domestic domains, Williams Adley applied a second filter to reflect enabled accounts. A third filter was then applied to reflect accounts that were not expired, which yielded a population of 40,794 domestic accounts. From a population of 40,794 domestic accounts, Williams Adley filtered the list to reflect accounts that had not been used for more than 90 days, which yielded 2,601 results. Therefore, Williams Adley determined that 2,601 domestic accounts were inactive for more than 90 days and had not been disabled from the Department's Active Directory, as required by the Foreign Affairs Handbook.

¹⁶ (U) Bureau of Information Resource Management, Department Notice 2015_06_079, "Introduction of Badge Login to OpenNet for Domestic Offices," June 10, 2015.

(SBU) Table A.1: Foreign and Domestic Domains in Active Directory

Domain	Foreign	Domestic	Population of Domestic Accounts
af.state.sbu	X		-
appservices.state.sbu		X	1,484
ca.state.sbu		X	9,163
conus.state.sbu		X	402
ds.state.sbu		X	6,507
eap.state.sbu	X		-
eur.state.sbu	X		-
gfs.state.sbu		X	1,025
neasa.state.sbu	X		-
oig.state.sbu		X	478
ses.state.sbu		X	1,158
state.sbu		X	68
washdc.state.sbu		X	20,509
wha.state.sbu	X		-
Total	5	9	40,794

Source: Generated by Williams Adley from data provided by the Department.

(U) APPENDIX B: BUREAU OF INFORMATION RESOURCE MANAGEMENT RESPONSE



United States Department of State

Washington, D.C. 20520

~~SENSITIVE BUT UNCLASSIFIED~~
(UNCLASSIFIED when separated from Attachment)

April 25, 2016

INFORMATION MEMO FOR ASSISTANT IG BROWN (OIG/AUD)

FROM: IRM/PDCIO – Frontis B. Wiggins *FBW*

SUBJECT: (U) Management Assistance Report: Inactive Accounts within the
Department of State's Active Directory

(SBU) I thank you for the opportunity to respond to the aforementioned report. Active Directory health is one component of our efforts to strengthen our cybersecurity efforts. As noted in the report, IRM has begun an effort to focus our attention on those users with the most access to OpenNet – our privileged users. Our efforts include reducing the number of privileged users, improve the process whereby these users get accounts, and lighten the management of application specific privileged accounts.

(SBU) As for all other OpenNet users, we routinely delete stale accounts. Our Information Assurance Directorate continues to conduct a monthly scrub of inactive accounts and started with our overseas accounts first. They expect to move to the domestic accounts soon and then conduct routine maintenance thereafter.

(SBU) We appreciate your continued support and assistance in improving the Department's cybersecurity posture. If you have any questions, please contact Jameela Raja Akbari, Senior Management Advisor, External Affairs, by email at [REDACTED]@state.gov.

Attachment:

Tab – IRM Response to Management Assistance Report: Inactive Accounts
within the Department of State's Active Directory

~~SENSITIVE BUT UNCLASSIFIED~~
(UNCLASSIFIED when separated from Attachment)

Recommendation 1: ~~(SBU)~~ OIG recommends that the Bureau of Information Resource Management amend the “Program Management Plan for PIV Login to OpenNet Deployment” to address the identification and removal process of mailbox, service, and terminated user accounts.

Management Response (April 2016): ~~(SBU)~~ IRM non-concurs with this recommendation. The Program Management Plan for PIV Login was created to deploy and implement PIV domestically and overseas. Now that IRM has completed that goal, the plan has been completed and does not lend itself to amendment.

~~(SBU)~~ IRM has begun an effort to focus our attention on those users with the most access to OpenNet – our privileged users. Our efforts include reducing the number of privileged users, improve the process whereby these users get accounts, and tighten the management of application specific privileged accounts. We continue to routinely delete stale accounts. Our Information Assurance Directorate continues to conduct a monthly scrub of inactive accounts.

Recommendation 2: ~~(SBU)~~ OIG recommends that the Bureau of Information Resource Management implement the new guidance from the “Program Management Plan for PIV Login to OpenNet Deployment,” once amended in response to Recommendation 1 of this report.

Management Response (April 2016): ~~(SBU)~~ IRM non-concurs with this recommendation. The Program Management Plan for PIV Login was created to deploy and implement PIV domestically and overseas. Now that IRM has completed that goal, the plan has been completed and does not lend itself to amendment.

~~(SBU)~~ IRM has begun an effort to focus our attention on those users with the most access to OpenNet – our privileged users. Our efforts include reducing the number of privileged users, improve the process whereby these users get accounts, and tighten the management of application specific privileged accounts. We continue to routinely delete stale accounts. Our Information Assurance Directorate continues to conduct a monthly scrub of inactive accounts.



HELP FIGHT FRAUD. WASTE. ABUSE.

1-800-409-9926

[OIG.state.gov/HOTLINE](https://oig.state.gov/HOTLINE)

If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:

OIGWPEAOmbuds@state.gov

oig.state.gov

Office of Inspector General • U.S. Department of State • P.O. Box 9778 • Arlington, VA 22219