



OIG

Office of Inspector General

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

AUD-IT-IB-16-36

Office of Audits

May 2016

(U) Management Assistance Report: Inactive User Accounts Within the Broadcasting Board of Governors 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 Broadcasting Board of Governors (BBG) uses a Microsoft for Windows directory service known as Active Directory (AD) to centrally manage network users, groups, and system information while enforcing BBG's security standards and standardizing network configuration. AD allows assignment of access controls to individuals and services based on their respective roles. Acting on behalf of the Office of Inspector General, Office of Audits, Williams, Adley & Company-DC, LLP (Williams Adley), an independent public accounting firm, evaluated whether BBG 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. BBG's Identification and Authentication Policy states that BBG officials should disable inactive user accounts after 45 or more days. AD accounts tested for this audit were generated on January 5, 2016.

~~(SBU)~~ Williams Adley found it difficult to determine the number of inactive user accounts because BBG had incorrectly identified other types of accounts as user accounts in AD. For example, of 2,788 accounts that BBG presented as user accounts, Williams Adley identified 132 accounts (5 percent) that were not user accounts, including service, shared, and training student accounts. Service accounts are non-user accounts that are used to run particular services on applications and servers. Shared and training student accounts are used by multiple users to access particular resources, such as training classes. These non-user accounts were incorrectly identified as user accounts in part because BBG's Identification and Authentication Policy does not contain sufficient guidance regarding how to maintain different types of accounts in AD.

~~(SBU)~~ Once Williams Adley was able to determine the actual population of user accounts (2,656), it found that BBG generally disabled inactive user accounts in AD after 45 days of inactivity, as prescribed in its policy. Of 2,656 user accounts evaluated, Williams Adley identified only 8 inactive accounts (less than 1 percent) that had not been disabled. The eight exceptions identified were privileged accounts, which are user accounts with elevated access rights. According to a BBG official, privileged accounts are not treated as regular user accounts because users of privileged accounts do not log in on a regular basis. In addition, Williams Adley found that BBG does not have a policy for disabling other types of inactive accounts, such as service, shared, and training student accounts.

(U) Addressing these weaknesses is important because, if an intruder gains access to a privileged account that has elevated administrative rights, the intruder can access personally identifiable information, which significantly increases the risk that BBG's confidential information could be altered or stolen. Further, ineffective AD account management of non-user accounts increases the risk of unauthorized access to BBG's information system applications and servers.

(U) In its April 19, 2016, response (see Appendix B) to a draft of this report, BBG concurred with the recommendations to revise the Identification and Authentication Policy; therefore, OIG considers the recommendations resolved, pending further action. BBG'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 BBG disabled inactive AD user accounts after 45 days, as required by its internal policies.

(U) BACKGROUND

(U) BBG is an independent Federal agency that supervises all U.S. civilian international broadcasting. BBG broadcasters distribute programming in 61 languages to an estimated weekly audience of 215 million people via radio, television, the internet, and other news media. As such, BBG depends on information systems and electronic data to carry out essential mission-related functions, the security of which is vital to ensuring the continued operations of BBG. As an organization with international exposure, BBG's information systems are subject to serious threats that can have adverse effects on organizational operations, assets, and individuals.

(U) Access to organizational data is controlled through identity and access management. 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 BBG 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 BBG's security standards and standardizing network configuration. 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) Prior OIG Reports

(U) Since FY 2010, OIG repeatedly has reported deficiencies in BBG's identity and access management, specifically regarding account management. For example, as a result of mandated Federal Information Security Management Act audits,² OIG reported deficiencies with BBG's AD that included the following:

- (U) BBG did not implement effective password management policies requiring the use of complex passwords for sufficient user verification.
- (U) User accounts were not disabled timely in accordance with BBG's Identification and Authentication policy.

(U) RESULTS

~~(SBU)~~ According to the National Institute of Standards and Technology,³ inactive accounts should be automatically disabled after a defined period of time. BBG's Identification and Authentication Policy⁴ states that BBG officials should disable inactive user accounts after 45 or more days. It was difficult for Williams Adley to determine the number of inactive user accounts because BBG had incorrectly identified service, shared, and training student accounts as user accounts in AD. Service accounts are non-user accounts that run particular services on applications and servers. Shared and training student accounts are non-user accounts that are used by multiple users to access particular resources, such as training classes.

~~(SBU)~~ Once Williams Adley was able to determine the population of user accounts, it found that BBG was generally disabling inactive AD user accounts in 45 days or less in accordance with its internal policies. Specifically, Williams Adley found only 8 (less than 1 percent) of 2,656 user accounts that were inactive for more than 45 days and had not been disabled in AD. AD accounts tested for this audit was generated on January 5, 2016 (see Appendix A for a detailed description of the scope and methodology). The eight accounts identified remained open after more than 45 days of inactivity primarily because these accounts were privileged accounts, which are user accounts with elevated access rights. Such accounts are used to log onto workstations and servers to perform administrative duties such as installing software and

² (U) OIG, *Review of the Information Security Program at the Broadcasting Board of Governors* (AUD-IT-IB-11-08, November 2010), *Evaluation of the Broadcasting Board of Governors Information Security Program* (AUD-IT-IB-12-15, November 2011), *Audit of the Broadcasting Board of Governors Information Security Program* (AUD-IT-IB-13-04, November 2012), *Audit of the Broadcasting Board of Governors Information Security Program* (AUD-IT-IB-14-02, October 2013), *Audit of the Broadcasting Board of Governors Information Security Program* (AUD-IT-IB-15-13, October 2014), and *Audit of the Broadcasting Board of Governors Information Security Program* (AUD-IT-IB-16-17, November 2015).

³ (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.

⁴ (U) BBG's Office of Technology, Services, and Innovation, Identification and Authentication Policy, April 1, 2011 (last updated March 27, 2012).

troubleshooting issues. According to a BBG official, privileged accounts are not treated as regular user accounts because users of privileged accounts do not log in on a regular basis. BBG's Identification and Authentication Policy does not distinguish between different types of user accounts.

(U) In addition to the issues identified with user accounts, Williams Adley found that BBG's Identification and Authentication Policy does not define a time period for disabling non-user accounts. According to a BBG official, BBG is developing a policy for non-user accounts, which will include a timeframe to disable these accounts. BBG officials stated that BBG plans to have the policy implemented by early 2016.

(U) These issues are important to address because, if an intruder gains access to a privileged account that has elevated administrative rights, the intruder can access personally identifiable information, which significantly increases the risk that BBG's confidential information could be altered or stolen. Further, ineffective AD account management of non-user accounts increases the risk of unauthorized access to BBG's information system applications and servers, which could impede BBG's ability to achieve its core mission.

Recommendation 1: (U) OIG recommends that the Chief Information Officer for the Broadcasting Board of Governors revise the Identification and Authentication Policy to provide guidance on how to identify and segregate user and non-user accounts in Active Directory.

(U) Management Response: BBG concurred with this recommendation, stating that it will revise its Identification and Authentication Policy to provide guidance on how to identify and segregate user and non-user accounts.

(U) OIG Reply: OIG considers this recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that BBG revised its Identification and Authentication Policy to provide guidance on how to identify and segregate user and non-user accounts in AD.

Recommendation 2: (U) OIG recommends that the Chief Information Officer for the Broadcasting Board of Governors revise the Identification and Authentication Policy to define when privileged user accounts in Active Directory become inactive and must be disabled.

(U) Management Response: BBG concurred with this recommendation, stating that it will revise its Identification and Authentication Policy to more clearly define when privileged user accounts become inactive and must be disabled.

(U) OIG Reply: OIG considers this recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation

demonstrating that BBG revised its Identification and Authentication Policy to define when privileged user accounts in AD become inactive and must be disabled.

Recommendation 3: (U) OIG recommends that the Chief Information Officer for the Broadcasting Board of Governors revise the Identification and Authentication Policy to define when non-user accounts in Active Directory become inactive and must be disabled.

(U) Management Response: BBG concurred with this recommendation, stating that it will revise its Identification and Authentication Policy to more clearly define when non-user accounts become inactive and must be disabled.

OIG Reply: (U) OIG considers this recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that BBG revised its Identification and Authentication Policy to define when non-user accounts in AD become inactive and must be disabled.

(U) RECOMMENDATIONS

Recommendation 1: (U) OIG recommends that the Chief Information Officer for the Broadcasting Board of Governors revise the Identification and Authentication Policy to provide guidance on how to identify and segregate user and non-user accounts in Active Directory.

Recommendation 2: (U) OIG recommends that the Chief Information Officer for the Broadcasting Board of Governors revise the Identification and Authentication Policy to define when privileged user accounts in Active Directory become inactive and must be disabled.

Recommendation 3: (U) OIG recommends that the Chief Information Officer for the Broadcasting Board of Governors revise the Identification and Authentication Policy to define when non-user accounts in Active Directory become inactive and must be disabled.

(U) APPENDIX A: SCOPE AND METHODOLOGY

~~(SBU)~~ The Broadcasting Board of Governors (BBG) provided three system-generated listings comprising all BBG Active Directory^[1] (AD) accounts for January 5, 2016, which contained service accounts,^[2] privileged accounts,^[3] and other accounts. The three listings are shown in Table A.1.

~~(SBU)~~ Table A.1: Active Directory Listings

| Listing Name | Population |
|---------------------|-------------------|
| Service Accounts | 70 |
| Privileged Accounts | 119 |
| Accounts | 2,767 |
| Total | 2,956 |

Source: Generated by Williams Adley based on BBG AD data.

~~(SBU)~~ Williams, Adley & Company-DC, LLP (Williams Adley), inspected the service account listing and determined that no user accounts were contained in the listing. Therefore, Williams Adley did not include this listing in the population for this audit (which focused exclusively on user accounts).

~~(SBU)~~ Williams Adley compared the two remaining AD listings (Privileged Accounts and Accounts), which BBG identified as including user accounts, to determine whether there were any duplicate records. Williams Adley identified 98 records that were duplicated, yielding 2,788 unique accounts. Then Williams Adley inspected the remaining accounts to ensure that the accounts were user accounts. Specifically, Williams Adley assessed the account names based on BBG's AD naming convention for user accounts. Based on an inspection of the 2,788 accounts, Williams Adley determined that 132 accounts were not user accounts; therefore, the population of user accounts reviewed was 2,656.

^[1] (U) Per TechNet, AD is a directory service created by Microsoft for the Windows domain network, which provides the capability to centrally manage network users and system information while enforcing BBG's security standards and standardizing network configuration. See <[https://technet.microsoft.com/en-us/library/cc759073\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx)>, accessed on January 14, 2016.

^[2] (U) Service accounts are non-user accounts that run particular services on applications and servers.

^[3] (U) Privileged accounts, such as workstation administrator and server administrator accounts, are user accounts with elevated access rights. They are used to log onto workstations and servers to perform administrative duties such as installing software and troubleshooting issues.

(U) APPENDIX B: BROADCASTING BOARD OF GOVERNORS RESPONSE



Broadcasting Board of Governors
United States of America

April 18, 2016

Mr. Norman P. Brown
Assistant Inspector General for Audits
Office of Inspector General
U.S. Department of State

Dear Mr. Brown:

Thank you for the opportunity to respond to the *Management Assistance Report: Inactive User Accounts Within the Broadcasting Board of Governors Active Directory*.

The Agency concurs with the report's recommendations that the Chief Information Officer revise the Identification and Authentication Policy to (1) provide guidance on how to identify and segregate user and non-user accounts, (2) more clearly define when privileged user accounts become inactive and must be disabled, and (3) more clearly define when non-user accounts become inactive and must be disabled. BBG Active Directory account policies, procedures, and workflows are being modified as necessary.

Please do not hesitate to contact us should you have questions.

Sincerely,

A handwritten signature in black ink, which appears to read "John F. Lansing", is positioned above the typed name.

John F. Lansing
Chief Executive Officer and Director



330 Independence Avenue, SW | Room 1300 | Cohen Building | Washington, D.C. 20237 | (202) 203-4545 | Fax (202) 203-4568

Recommendation 1. OIG recommends that the Chief Information Officer for the Broadcasting Board of Governors revise the Identification and Authentication Policy to provide guidance on how to identify and segregate user and non-user accounts in Active Directory.

BBG Response: Concur. The BBG will revise its Identification and Authentication Policy to provide guidance on how to identify and segregate user and non-user accounts.

Recommendation 2. OIG recommends that the Chief Information Officer for the Broadcasting Board of Governors revise the Identification and Authentication Policy to define when privileged user accounts in Active Directory become inactive and must be disabled.

BBG Response: Concur. The BBG will revise its Identification and Authentication Policy to more clearly define when privileged user accounts become inactive and must be disabled.

Recommendation 3. OIG recommends that the Chief Information Officer for the Broadcasting Board of Governors revise the Identification and Authentication Policy to define when non-user accounts in Active Directory become inactive and must be disabled.

BBG Response: Concur. The BBG will revise its Identification and Authentication Policy to more clearly define when non-user accounts become inactive and must be disabled.

~~SENSITIVE BUT UNCLASSIFIED~~



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

~~SENSITIVE BUT UNCLASSIFIED~~