NOAA Inadequately Managed Its Active Directories That Support Critical Missions

FINAL REPORT NO. OIG-22-018-A

FEBRUARY 3, 2022

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

February 3, 2022

MEMORANDUM FOR: Richard W. Spinrad, Ph.D.
Under Secretary of Commerce for Oceans and Atmosphere and
NOAA Administrator
National Oceanic and Atmospheric Administration

FROM: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *NOAA Inadequately Managed Its Active Directories That Support Critical Missions*
Final Report No. OIG-22-018-A

Attached for your review is our final report on the audit of the National Oceanic and Atmospheric Administration's (NOAA's) Active Directories. Our audit objective was to determine whether NOAA has adequately managed its Active Directories to protect mission critical systems and data.

We found the following:

I. Excessive privileges could increase the risk of a successful compromise.

II. Inadequately managed accounts provided more opportunities for cyberattacks.

III. End-of-life operating systems were vulnerable to security exploitation.

In a January 19, 2022, response to our draft report, NOAA concurred with our findings and recommendations and described actions they have taken, or will take, to address them. At the request of NOAA, the detailed information related to its specific systems has been removed in this final report. NOAA's complete response—which also included general comments—is included within the final report as appendix B.

Pursuant to Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendations in this report within 60 calendar days. This final report will be posted on the Office of Inspector General's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (5 U.S.C. App., §§ 4 & 8M).

We appreciate the cooperation and courtesies extended to us by your staff during our audit. If you have any questions or concerns about this report, please contact me at (202) 793-2938 or Dr. Ping Sun, Director for IT Security, at (202) 793-2957.

Attachment

cc: André Mendes, Chief Information Officer
Janet Coit, Assistant Administrator for NOAA Fisheries and Acting Assistant Secretary of Commerce for Oceans and Atmosphere and Deputy NOAA Administrator, NOAA
Karen Hyun, Chief of Staff, NOAA
Zachary Goldstein, Chief Information Officer, NOAA
James Jones, Director Cyber Security Division, NOAA
Tanisha Bynum-Frazier, Director, Audit and Information Management Office, NOAA
Brian Doss, Alternate Audit Liaison, NOAA
Lisa Lim, Alternate Audit Liaison, NOAA
Joselyn Bingham, Audit Liaison, OCIO
Maria Hishikawa, IT Audit Liaison, OCIO
Ryan Higgins, Chief Information Security Officer, OCIO
MaryAnn Mausser, Audit Liaison, Office of the Secretary

Report in Brief

February 3, 2022

Background

The U.S. Department of Commerce (the Department) and its bureaus are required to follow federal laws to secure information technology (IT) systems through the cost-effective use of managerial, operational, and technical controls. This responsibility applies to all federal IT systems, including National Oceanic and Atmospheric Administration (NOAA) systems.

NOAA's mission is to understand and predict changes in climate, weather, oceans, and coasts; to share that knowledge and information with other agencies and the public; and to conserve and manage coastal and marine ecosystems and resources. The agency's information systems and applications are crucial to reliably support its national critical mission—providing hazardous weather forecasts and warnings—which are essential in protecting life, property, and the nation's economy.

Active Directories—critical components of NOAA IT infrastructure—maintain logical structures, known as domains, to manage all network resources. If deployed and managed properly, each Active Directory can provide a secure means to manage networked user accounts, workstations, servers, printers, and system configurations within its domain. Due to the nature of their role, Active Directories hold sensitive information, such as users' credentials and network topologies, making them prime targets for cyberattacks.

Why We Did This Review

Our audit objective was to determine whether NOAA has adequately managed its Active Directories to protect mission critical systems and data.

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

NOAA Inadequately Managed Its Active Directories That Support Critical Missions

OIG-22-018-A

WHAT WE FOUND

The audit focused on three selected Active Directories in three line offices that support NOAA's critical mission: the National Environmental Satellite, Data, and Information Service, the National Weather Service, and the National Marine Fisheries Service. To assess NOAA's Active Directories, we utilized a specialized Active Directory assessment tool. We evaluated fundamental security practices, relationships, and configurations to determine whether any deficiencies existed within each Active Directory.

We found that NOAA inadequately managed its Active Directories. Specifically, on all selected Active Directories, we identified accounts having excessive privileges, inadequate account management, as well as end-of-life operating systems running within the Active Directory domain. These deficiencies—whether standalone or combined—increase the risk of successful cyberattacks and jeopardize NOAA's ability to accomplish its mission.

WHAT WE RECOMMEND

We recommend that the Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator ensures that NOAA's Chief Information Officer does the following:

1. Establish processes and procedures to periodically review all Active Directory accounts to ensure consistent adherence to the principle of least privilege per Department policy.
2. Determine the feasibility of requiring all NOAA line offices to use specialized Active Directory security tool(s) to conduct periodic reviews.
3. Establish procedures to periodically review Active Directory accounts, passwords, groups, and Group Policy Objects for compliance with account management requirements as stated in the Department's policy and following industry best practices. If feasible, utilize specialized Active Directory security tool(s) to conduct periodic reviews.
4. Establish policies or procedures to require compensating controls for service accounts that cannot have regular password changes.
5. Establish decommission plans with milestones to prioritize and expedite the upgrading or retirement of computers with end-of-life operating systems.

Contents

Cover: Herbert C. Hoover Building main entrance at 14th Street Northwest in Washington, DC. Completed in 1932, the building is named after the former Secretary of Commerce and 31st President of the United States.

Introduction

The U.S. Department of Commerce (the Department) and its bureaus are required to follow federal laws to secure information technology (IT) systems[1] through the cost-effective use of managerial, operational, and technical controls. This responsibility applies to all federal IT systems, including National Oceanic and Atmospheric Administration (NOAA) systems.

NOAA's mission is to understand and predict changes in climate, weather, oceans, and coasts; to share that knowledge and information with other agencies and the public; and to conserve and manage coastal and marine ecosystems and resources. The agency's information systems and applications are crucial to reliably support its national critical mission—providing hazardous weather forecasts and warnings—which are essential in protecting life, property, and the nation's economy.

Active Directories—critical components of NOAA IT infrastructure—maintain logical structures, known as *domains*,[2] to manage all network resources. If deployed and managed properly, each Active Directory can provide a secure means to manage networked user accounts, workstations, servers, printers, and system configurations within its domain, as illustrated in figure 1. Due to the nature of their role, Active Directories hold sensitive information, such as users' credentials and network topologies, making them prime targets for *cyberattacks*.[3]

Figure 1. The Concept of Active Directory

Source: OIG

[1] See Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551, *et seq*.

[2] *Domain* is a networked group of users, workstations, servers, printers, software applications (e.g., databases and websites) as well as other network devices. Everything within the domain is controlled by the Active Directory.

[3] *Cyberattacks* relate to both successful and non-successful attempts to leverage and exploit vulnerabilities to compromise computers by malicious threat actors, which may result in negative impact to confidentiality, integrity, or availability.

Objective, Findings, and Recommendations

Our audit objective was to determine whether NOAA has adequately managed its Active Directories to protect mission critical systems and data. The audit focused on three selected Active Directories in three line offices that support NOAA's critical mission: the National Environmental Satellite, Data, and Information Service (NESDIS), the National Weather Service (NWS), and the National Marine Fisheries Service (NMFS). To assess NOAA's Active Directories, we utilized a specialized Active Directory assessment tool. We evaluated fundamental security practices, relationships, and configurations to determine whether any deficiencies existed within each Active Directory. Appendix A provides a more detailed description of our audit objective, scope, and methodology.

We found that NOAA inadequately managed its Active Directories. Specifically, on all selected Active Directories, we identified accounts having excessive *privileges*,[4] inadequate account management, as well as end-of-life (EOL) operating systems running within the Active Directory domain. These deficiencies—whether standalone or combined—increase the risk of successful cyberattacks and jeopardize NOAA's ability to accomplish its mission.

After providing NOAA system administrators, security staff, and management with the findings, they immediately began to take action. This cooperation allowed for remediation of deficiencies to start before the conclusion of our audit.

In addition, NOAA expressed a commitment to Active Directory security, including those Active Directories not selected for the audit. NOAA demonstrated explicit interest in the use of specialized security tools—utilized during the audit—to proactively identify similar Active Directory issues in other NOAA Active Directories. Furthermore, NOAA plans to create guidance documentation and compensating controls, which will support preemptive measures related to the security weaknesses identified in this report.

I. Excessive Privileges Could Increase the Risk of a Successful Compromise

One of the primary Active Directory roles is to manage user accounts' access privileges. To comply with the *least privilege* security principle, a National Institute of Standards and Technology control requirement,[5] each account must be given access privileges only to relevant function areas required by users' roles and responsibilities. When we analyzed Active Directory's configurations, we found excessive privileges given to accounts across all selected Active Directories from the three line offices. Specifically, we found (a) accounts possessed unneeded local administrative privileges and (b) accounts had unneeded

[4] *Privilege* defines the actions and functions users are allowed to do, such as installing and removing any software or modifying critical computer security settings.

[5] U.S. Department of Commerce National Institute of Standards and Technology, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4. Gaithersburg, MD: NIST, F-153. Available online at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (accessed October 8, 2021). (Withdrawn Sept. 23, 2021, and superseded by Revision 5).

privileges, such as remote access to computers and the ability to make unintended changes to security settings.

A. Accounts possessed unneeded local administrative privileges

We reviewed the three selected NOAA Active Directories and found 58 accounts having unneeded local administrative privileges on 202 computers (see table 1). Having local administrative privileges allows for full control over the computers, which also creates an at-risk environment for the entire Active Directory. For example, accounts with such privileges can install and remove any software, including those carrying malicious code, or modify critical computer security settings, such as disabling anti-virus software. Furthermore, users have full access to the data stored on these computers.

Table 1. Unneeded Local Administrator Rights

Line Office's Active Directory	No. of Accounts	No. of Computers
NESDIS	29	168
NWS	1	3
NMFS	28	31
Total	**58**	**202**

Source: OIG

The least privilege security principle is intended to lessen the impact of successful attacks. Hijacking a privileged user account is extremely favorable for attackers as it possesses more access rights and, therefore, has a higher chance of compromising critical systems.

The same principle also allows for greater system and network stability as software applications and files cannot be deleted or misconfigured by additional users who do not require access. More importantly, security of sensitive data is improved when user accounts are only allowed to access what is minimally required.

The main cause for this deficiency was misconfiguration of accounts and the lack of regular review of account privileges. We provided the results of our assessment to all three NOAA offices, and each office began implementing corrective actions during our audit. Specifically, NESDIS developed a Configuration Change Request (CCR) action[6] to review identified privileged accounts and remediate when necessary. NWS immediately disabled the one affected account. NMFS either deleted, disabled, flagged as pending deletion, or revoked the privileges of the 28 accounts.

[6] A *CCR action* is the process for documenting and managing the change and configuration of components connected to the NESDIS system. Each step is fully recorded in a configuration management plan and change control process. Thus, the end product created is called a "Configuration Change Request."

B. Accounts had unneeded privileges, such as remote access to computers and the ability to make unintended changes to security settings

Active Directory users and groups are typically assigned specific access privileges for system and network resources such as computers, printers, and other Active Directory objects.[7] We reviewed the selected Active Directories and found 12 users who had unneeded privileges, such as full rights to the Active Directory object and remote desktop protocol (RDP) access (see table 2).

Table 2. Unneeded Privileges

Line Office's Active Directory	No. of Accounts
NESDIS	1
NWS	0
NMFS	11
Total	**12**

Source: OIG

We found six accounts on NMFS Active Directory having full Active Directory rights, which allows users to make any changes to the associated Active Directory object, such as adding users to a group or resetting users' passwords. NMFS confirmed that these privileges were unneeded and removed them from the accounts immediately.

We also identified a total of six accounts on Active Directories from NESDIS and NMFS having unneeded RDP access privilege. This privilege allows users to login into a remote computer via a graphical interface, thus providing the user access to data and resources on the computer as if they were logging in locally. RDP has proven to be an area of interest for threat actors, as demonstrated by multiple DarkSide and REvil ransomware[8] attacks, which allowed these threat actors to gain unauthorized remote access through RDP to U.S. entities as well as worldwide companies' assets.[9] We provided the results

[7] Active Directory objects are items existing in the Active Directory. Common Active Directory objects include users, computers, applications, printers, and shared folders. These objects also have attributes. For example, a user object will have a person's name, department, and email address.

[8] *Ransomware* is defined as "an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption." *See* U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), "Ransomware 101" [online]. https://www.cisa.gov/stopransomware/ransomware-101 (accessed September 28, 2021). In 2021, the Federal Bureau of Investigation (FBI) and CISA issued a joint cybersecurity advisory about ransomware attacks, including those made by REvil. *See* DHS CISA, "Ransomware Awareness for Holidays and Weekends," alert (AA21-243A), August 31, 2021 [online]. https://us-cert.cisa.gov/ncas/alerts/aa21-243a (accessed October 8, 2021).

[9] John Martineau, "Understanding REvil: The Ransomware Gang Behind the Kaseya VSA Attack," July 6, 2021 [online]. https://unit42.paloaltonetworks.com/revil-threat-actors/ (accessed September 28, 2021).

of our assessment to the applicable NOAA offices, and they began correcting identified weaknesses during our audit.

The cause for these deficiencies was due to misconfiguration of accounts and the lack of regular review of Active Directories. In general, as users go through changes in their professional careers (such as being promoted, moving internally, or leaving the organization) the necessary changes to their account privileges should be correctly reflected. Therefore, it is imperative that Active Directory managers periodically review the Active Directory to prevent *privilege creep*[10] and to ensure accounts remain correctly configured at all times.

Excessive privileges can be exploited by attackers, allowing for *lateral movement*[11] from one compromised server to another on the network. In addition, attackers can exploit these rights to maintain *persistence*[12] on the network through remote code execution, which allows for the gathering of user credentials (username and password), impersonating other users, creating new user accounts, or disabling of security products installed on servers, such as anti-virus software. Consequently, the combination of these issues can significantly increase the risk of a successful compromise. Regular review of accounts and privileges could proactively prevent and minimize these security issues.

II. Inadequately Managed Accounts Provided More Opportunities for Cyberattacks

Account management embodies one of the most critical aspects of an organization's security posture because a single account can potentially act as a gateway to its IT resources and increase the risk of opportunity for a cyberattack. Account management includes following password policies and requirements, proper configuration, and actively removing or disabling inactive accounts. A well-known recent cyberattack on Colonial Pipeline's IT system leveraged an inactive user account,[13] among other vulnerabilities, which demonstrates the significance of effective account management.

We found inadequate account management on all selected NOAA's Active Directories. Specifically, we identified

a. enabled accounts never used within the last 60 days;

b. enabled accounts with passwords older than 90 days;

[10] *Privilege creep* is the gradual accumulation of access privileges beyond what an individual needs to do for their job function.

[11] *Lateral movement* is the tactic an adversary would utilize to move through a network to attempt to gain access to sensitive data.

[12] *Persistence* is a technique used by attackers to maintain their foothold on a system.

[13] Senate Republican Policy Committee, "Infrastructure Cybersecurity: Pipelines," policy paper, July 24, 2021 [online]. https://www.rpc.senate.gov/policy-papers/infrastructure-cybersecurity-pipelines (accessed October 4, 2021).

c. account passwords set to never expire;

d. no uniform password requirements for service accounts;

e. accounts misconfigured to have Service Principal Name enabled;

f. improper separation of user and privileged accounts; and

g. empty user groups and unused Group Policy Objects[14] (GPOs).

A. Accounts were enabled, but never used within the last 60 days

We reviewed accounts on selected Active Directories and identified 296 accounts that were enabled, but not used within the last 60 days (see table 3). This illustrates the fact that NOAA did not disable or remove inactive users as required by Department policy.[15] Keeping unnecessary inactive accounts increases the *attack surface*[16] and the risk of system compromise.

Table 3. Accounts Enabled but Not Used within Last 60 Days

Line Office's Active Directory	No. of Accounts
NESDIS	110
NWS	5
NMFS	181
Total	**296**

Source: OIG

Once provided the information, the line offices have begun to take corrective actions, which included disabling and deleting accounts. NESDIS confirmed that this finding was valid and planned to implement the CCR action to review the accounts and take corrective action, as necessary. NWS and NMFS disabled the 186 accounts associated with the finding.

The reason for the deficiency was largely due to inadequate reviews of the Active Directory. In addition, coronavirus disease 2019 (COVID-19) pandemic restrictions and mandatory office shutdowns enforcing maximum telework increased the level of difficulty for managing Active Directories across the agency. For example, automatic scripts to disable accounts after periods of inactivity were suspended temporarily to alleviate network access complications.

[14] GPOs contain specific configuration settings that are applied to groups of users and computers.

[15] Department Information Technology Security Baseline Policy (DOC ITSBP) requires user accounts to be disabled after 60 days of inactivity.

[16] *Attack surface* refers to the number of entry points exposed to a potential hacker.

B. *Accounts were logging on with passwords older than 90 days*

We found 48 accounts with passwords older than 90 days on Active Directories from NESDIS and NMFS (see table 4). NOAA failed to enforce password changes, as mandated by Department policy.[17] Infrequent password changes may increase the risk of *brute force*[18] attacks.

Table 4. Accounts with Passwords Older than 90 Days

Line Office's Active Directory	No. of Accounts
NESDIS	9
NWS	0
NMFS	39
Total	**48**

Source: OIG

Like finding II.A, the reason for the deficiencies was lack of adequate review of Active Directory accounts. Additionally, the impact of the COVID-19 maximum telework requirement placed a higher level of difficulty with managing user passwords on computers not continuously connected to the internal NOAA networks.

Password management plays a significant role in preventing successful cyberattacks from brute force attacks and use of stolen passwords. In 2019, Microsoft announced that 44 million accounts were vulnerable to account takeover because of compromised or stolen passwords.[19] Additionally, a survey conducted in 2019 by Google has shown that at least 65 percent of users reuse the same password for multiple accounts, thus significantly increasing the stolen password attack surface.[20] Both NESDIS and NMFS have planned and taken action to remediate the accounts.

C. *Accounts passwords were set to never expire*

NOAA had set passwords to never expire on Active Directory accounts in situations where multifactor authentication (MFA) was implemented or when necessary to support operations, such as service accounts or emergency-use accounts. However, we identified 102 user accounts misconfigured to have passwords set to never expire on

[17] DOC ITSBP requires passwords to be changed every 90 days.

[18] *Brute force* password attacks involve trying all possible combinations to find a match.

[19] Davey Winder, "Microsoft Security: Password Problem Affecting 44 Million Users Revealed," December 6, 2019 [online]. https://www.forbes.com/sites/daveywinder/2019/12/06/microsoft-finds-password-security-problem-affecting-44-million-users/?sh=4aae221b67c4 (accessed October 4, 2021).

[20] Google, & Harris Poll, "Online Security Survey" February, 2019 [online]. https://services.google.com/fh/files/blogs/google_security_infographic.pdf (accessed September 16, 2021).

Active Directories from NESDIS and NMFS (see table 5). These accounts did not utilize MFA nor were deemed necessary to have never expiring passwords for operational needs.

Table 5. Accounts with Passwords Set to Never Expire

Line Office's Active Directory	No. of Accounts
NESDIS	8
NWS	0
NMFS	94
Total	**102**

Source: OIG

Non-expiring passwords could increase the risk of a cyberattack as described in finding II.B. Once we informed the associated NOAA offices with the identified accounts, NOAA promptly planned remediation of the issue.

D. No uniform password requirements were established for service accounts

Service accounts are generally not used by regular users. Rather, they are used by software applications running within Windows operating system environment, known as services, such as web or email servers. The service accounts, usually given higher privileges, act as a security identity to grant access to local and network resources, and allow Active Directory administrators to manage the associated running applications. Therefore, any compromised service accounts could result in a detrimental consequence to IT operations.

We identified 356 service accounts with never-expired passwords on selected Active Directories (see table 6), which violated the password requirements within the Department policy.[21] As we discussed prior in this report, infrequent password changes could increase successful attacks. While NOAA utilized service accounts with never-expired passwords to support critical operations, it did not have uniform policies or procedures in place that require compensating controls to ensure service accounts are adequately protected.

[21] DOC ITSBP policy requires passwords to be changed every 90 days.

Table 6. Service Accounts with Unexpired Passwords

Line Office's Active Directory	No. of Accounts
NESDIS	14
NWS	6
NMFS	336
Total	**356**

Source: OIG

Since NOAA has no uniform policy or procedure, NOAA allowed units to assume an ad hoc approach of adopting an additional requirement for service accounts. NMFS, for example, plans to implement a long passphrase for service accounts, which is a step toward securing service accounts.

E. Accounts were misconfigured to have service principal name (SPN) enabled and susceptible to specific cyberattack

Kerberoastable accounts are accounts that are configured to have SPNs, which is a Microsoft feature necessary to run services. Attackers can abuse this feature to gain the password of a Kerberoastable account and use it to gain unauthorized access to the server. This technique is called *Kerberoasting*.[22] We found 23 Kerberoastable accounts on Active Directories from NWS and NMFS (see table 7). To limit the risk of Kerberoasting, the recommended best practice is to limit accounts with SPNs (Kerberoastable) to minimally required rights and remove the SPNs when not needed.

Table 7. Kerberoastable Accounts

Line Office's Active Directory	No. of Accounts
NESDIS	0
NWS	1
NMFS	22
Total	**23**

Source: OIG

After providing the assessment results, both NWS and NMFS remediated all 23 accounts.

[22] Kerberoasting is identified as one of the well-known adversarial attacks by MITRE in its ATT&CK knowledge base (Attack ID: T1208). See MITRE, "Steal or Forge Kerberos Tickets: Kerberoasting," October 20, 2020 [online]. https://attack.mitre.org/techniques/T1208/ (accessed September 2, 2021).

F. Improper separation of user and privileged accounts existed

In general, the Active Directory selected for review within NESDIS contains two types of user accounts: (1) non-privileged accounts for regular purposes, such as email and office work, and (2) privileged accounts for administrative functions.[23] Using a separate privileged account for administrative functions adds an extra layer of defense against cyberattacks. For example, when a user becomes a victim of a *phishing*[24] attack, the user's account becomes compromised, and the attacker assumes all of the user's rights. When the compromised account has rights to perform administrative functions, it would allow an attacker to use these rights and potentially gain further access to systems and networks.

We identified 22 privileged users, including three domain administrators, that did not have regular purpose accounts to perform job functions on NESDIS Active Directory (see table 8). The use of privileged accounts to perform non-administrative job functions, and in general, the lack of non-privileged accounts for these 22 users elevates the risk to NOAA's IT security posture.

Table 8. Improperly Separated Accounts

Line Office's Active Directory	No. of Users
NESDIS	22
NWS	0
NMFS	0
Total	**22**

Source: OIG

A domain administrator account has full administrative privileges by default on all managed servers and computers within the Active Directory. Compromise of this account could potentially lead to the compromise of the entire Active Directory domain. Real-life illustrations of what can happen when a privileged Active Directory account is compromised are the multiple DarkSide and REvil ransomware cyberattacks, as previously discussed in finding I.B. For example, REvil threat actors compromised domain Active Directory administrator accounts to gain full administrator privileges. Then they remotely executed the ransomware on the targeted computers, resulting in the encryption of files from more than 60 service providers and more than

[23] Examples of administrative functions are resetting passwords of other users or changing their group membership and therefore modifying access rights.

[24] *Phishing* is a technique used to trick account users into disclosing sensitive data, such as credentials, through fraudulent solicitation. Often the attacker uses authentic-looking emails to request information or direct to a fake website.

1,500 businesses worldwide.[25] The threat actors then placed million-dollar ransoms to receive a decryption key and prevent the leaking of stolen files. Victims of ransomware attacks incur many financial damages, including but not limited to: payment of the ransom (which does not guarantee the release of files or removal of the malware), loss of sensitive or proprietary information, disruption to regular operations, system and file restoration, as well as reputational damages.[26]

Department policy requires employment of the least privilege principle and the use of non-privileged accounts or roles, when such privileges are not needed. NESDIS was unable to provide a reason for why privileged users had multiple privileged accounts and lacked non-privileged accounts. However, in response to our finding, NESDIS planned to conduct a comprehensive Active Directory account review to ensure compliance with all applicable policies, guidance, and best practices.

G. Empty user groups and unused GPOs

Within an Active Directory structure, accounts are usually organized into separate groups with varying permission levels. GPOs contain specific configuration settings that are applied to groups of users and computers. For example, a GPO can define password requirements such as specific length and complexity and apply them towards a group of specific users. Empty groups contain no accounts and unused GPOs are not applied to any groups of users and computers, therefore both should not be present in Active Directory.

We found 166 empty groups and 734 unused GPOs on all selected Active Directories (see table 9). Keeping these groups and GPOs may lead to unnecessary privileges being assigned to user accounts. For example, if an account is accidentally added to the wrong GPO or group, then it may have unintended elevated permissions or network access. Furthermore, keeping empty groups and unused GPOs may contribute to a disorganized and cluttered Active Directory, thereby making it more difficult to manage.

Table 9. Empty Groups and Unused GPOs

Line Office's Active Directory	No. of Groups	No. of GPOs
NESDIS	44	8
NWS	36	22
NMFS	86	704
Total	**166**	**734**

Source: OIG

[25] Lawrence Abrams, "REvil ransomware is back in full attack mode and leaking data," September 11, 2021 [online]. https://www.bleepingcomputer.com/news/security/revil-ransomware-is-back-in-full-attack-mode-and-leaking-data/ (accessed September 30, 2021).

[26] UC Berkeley, "What is the possible impact of Ransomware?" [online]. https://security.berkeley.edu/faq/ransomware/what-possible-impact-ransomware (accessed September 30, 2021).

After providing the assessment results to NESDIS, NWS, and NMFS, they immediately took action to review and remove groups and GPOs as necessary. NESDIS created a CCR to review all of our audit findings and remediate them when necessary. NWS and NMFS remediated all the empty groups and are in the process of remediating the GPOs we identified.

III. EOL Operating Systems Were Vulnerable to Security Exploitation

Keeping systems and their software products up-to-date is extremely important for security. EOL system components often have critical security flaws due to discontinued technical support and security updates from the manufacturers. As noted by the U.S. Department of Homeland Security's CISA, "Continued use of EOL software poses consequential risk to your system that can allow an attacker to exploit security vulnerabilities."[27]

We found 739 computers utilizing EOL operating systems (see table 10) on all selected Active Directories. Department policy requires the bureaus to manage and fund replacements for EOL hardware and software. Inactive computers no longer utilized should be removed from service.

Table 10. EOL Operating Systems

Line Office's Active Directory	No. of Systems
NESDIS	148
NWS	3
NMFS	588
Total	**739**

Source: OIG

The reasons for this deficiency were due to (1) the lack of timely removal of inactive computers, (2) hardware and software limitations, and (3) COVID-19 telework requirements placing limitations on remote updates. In response to our finding, NOAA began to take corrective actions. Specifically, NESDIS is currently in the process of drafting the decommissioning plan for appropriate approvals. NWS has already removed all 3 systems. Lastly, NMFS plans to remediate 576 systems and address 9 others. The remaining 3 NMFS computers require legacy operating systems for scientific equipment.

[27] DHS CISA. "Security Tip (ST04-006) Understanding Patches and Software Updates," February 1, 2021 [online]. https://cisa.gov/tips/st04-006 (accessed September 1, 2021).

Conclusion

In conclusion, the findings presented in this report, whether individually or combined, suggest NOAA Active Directories have a significantly increased risk of successful cyberattacks. This illustrates the need for periodic evaluations of all NOAA Active Directories to identify and quickly remediate weaknesses. We commend NOAA for taking prompt action to remediate the issues we identified during our audit and encourage taking proactive measures in securing all Active Directories NOAA-wide.

Recommendations

We recommend that the Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator ensures that NOAA's Chief Information Officer does the following:

1. Establish processes and procedures to periodically review all Active Directory accounts to ensure consistent adherence to the principle of least privilege per Department policy.
2. Determine the feasibility of requiring all NOAA line offices to use specialized Active Directory security tool(s) to conduct periodic reviews.
3. Establish procedures to periodically review Active Directory accounts, passwords, groups, and GPOs for compliance with account management requirements as stated in the Department's policy and following industry best practices. If feasible, utilize specialized Active Directory security tool(s) to conduct periodic reviews.
4. Establish policies or procedures to require compensating controls for service accounts that cannot have regular password changes.
5. Establish decommission plans with milestones to prioritize and expedite the upgrading or retirement of computers with EOL operating systems.

Summary of Agency Response and OIG Comments

On January 19, 2022, we received NOAA's responses to our draft report. In response to our draft report, NOAA concurred with all of our recommendations and described actions they have taken, or will take, to address them. At the request of NOAA, the detailed information related to its specific systems has been removed in this final report. NOAA's complete response—which also included general comments—is included within this report as appendix B.

We are pleased that NOAA concurs with our recommendations and look forward to receiving an action plan that will provide details on their corrective actions.

Appendix A: Objective, Scope, and Methodology

Our audit objective was to determine whether NOAA has adequately managed its Active Directories to protect mission critical systems and data.

The scope of this audit included three Active Directories selected from the three line offices that support NOAA's critical mission:

- National Environmental Satellite, Data, and Information Service (NESDIS) provides secure and timely access to global environmental data and information from satellites and other sources to promote and protect the nation's security, environment, economy, and quality of life. NESDIS data is used for monitoring environmental changes in real-time for early warning capabilities during environmental emergencies for the U.S. government.
- National Weather Service (NWS) provides weather, water, and climate data, forecasts, warnings, and impact-based decision support services for the protection of life and property and enhancement of the national economy.
- National Marine Fisheries Service (NMFS) is responsible for the stewardship of the nation's ocean resources and their habitat. In addition, it provides an ecosystem-based approach to management of sustainable fisheries and safe sources of seafood.

To accomplish our objective, we performed the following actions:

- Selected 11 out of over 80 Active Directories for a preliminary survey. Based on the survey, we selected 3 for an in-depth review;
- Used a specialized, open-source Active Directory assessment tool (BloodHound) to collect data from selected Active Directories and conducted an evaluation based on the collected data;
- Conducted assessments in accordance with NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*;
- Shared our initial assessment results with NESDIS, NWS, and NMFS staff; and
- Validated findings based off responses provided by NOAA.

We collected computer-generated data directly from NOAA's Active Directories. We verified this data by interviewing appropriate NOAA officials and provided them with the data to eliminate the possibility of false positive results. We determined that the data were sufficiently reliable for the purposes of this report.

We reviewed NOAA's compliance with the following applicable internal controls, provisions of law, and mandatory guidance:

- The Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551, *et seq*.
- U.S. Department of Commerce, *Information Technology Security Baseline Policy*
- NIST Special Publications:
  - 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
  - 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

We also used industry best practices as criteria for the review and testing of proper Active Directory configuration.

We conducted our review from November 2020 through September 2021 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. App.), and Department Organization Order 10-13, dated April 26, 2013, as amended October 21, 2020. We performed our work solely at remote telework locations.

We conducted this performance audit in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on its audit objective.

Appendix B: Agency Response

UNITED STATES DEPARTMENT OF COMMERCE
Deputy Under Secretary for Operations
National Oceanic and Atmospheric Administration
Washington, D.C. 20230

JAN 19 2022

MEMORANDUM FOR: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

FROM: Ben Friedman
Deputy Under Secretary for Operations
National Oceanic and Atmospheric Administration

SUBJECT: *NOAA Inadequately Managed Its Active Directories That Support Critical Missions*
Draft Report

The Department of Commerce's National Oceanic and Atmospheric Administration (NOAA) is pleased to submit the attached response to the draft report on NOAA's Active Directory. We reviewed the report and concurred with the recommendations.

Although NOAA agrees with the OIG's recommendations and findings, we strongly believe that the OIG draft report contains information about systems that is too specific for a publicly available report. Along with recent DOC security briefings that NOAA has attended, we believe that including the current level of detail in a public OIG report will increase the possibility that individuals may use information in the report to target and negatively impact NOAA systems used to support critical functions, including forecasts for severe weather events. We respectfully request that the OIG remove specific details from the publicly available report such as descriptions of NOAA Active Directories, and instead only note that the OIG generally reviewed systems at the National Weather Service, National Environmental Satellite, Data, and Information Service, and the National Marine Fisheries Service.

We appreciate the opportunity to review and respond to your draft report. If you have any questions please contact Tanisha Bynum-Frazier, Director, Audit and Information Management Office at 301-467-0832.

Department of Commerce National Oceanic and Atmospheric Administration Comments to the OIG Draft Report Titled "NOAA Inadequately Managed Its Active Directories That Support Critical Missions" December 2021

General Comments

The National Oceanic and Atmospheric Administration (NOAA) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report on NOAA's Active Directory entitled "NOAA Inadequately Managed Its Active Directories That Support Critical Missions." NOAA reviewed the draft report and concurs with the OIG's findings and recommendations. Our response to each recommendation and general comments are provided below.

We thank the OIG for highlighting areas for improvement and referencing specific tools to enhance our security posture. We are actively working to address the findings and are working on enterprise solutions that will help fully address findings and recommendations.

Although NOAA agrees with the OIG's recommendations and findings, we strongly believe that the OIG draft report contains information about systems that is too specific for a publicly available report. Along with recent DOC security briefings that NOAA has attended, we believe that including the current level of detail in a public OIG report will increase the possibility that individuals may use information in the report to target and negatively impact NOAA systems used to support critical functions, including forecasts for severe weather events. We respectfully request that the OIG remove specific details from the publicly available report such as descriptions of NOAA Active Directories, and instead only note that the OIG generally reviewed systems at the National Weather Service, National Environmental Satellite, Data, and Information Service, and the National Marine Fisheries Service.

NOAA Response to OIG Recommendations

Recommendation 1: That the Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator ensure that NOAA's Chief Information Office establish processes and procedures to periodically review all Active Directory accounts to ensure consistent adherence to the principle of least privilege per Department policy.

NOAA Response: We concur. NOAA is continuing to establish enterprise solutions and ultimately implement processes and procedures to ensure all NOAA systems adhere to all applicable DOC and NOAA policies.

Recommendation 2: That the Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator ensure that NOAA's Chief Information Office determine the feasibility of requiring all NOAA line offices to use specialized Active Directory security tool(s) to conduct periodic reviews.

NOAA Response: We concur. NOAA is working to identify and implement enterprise security tools under the Continuous Diagnostic and Mitigation (CDM) program for all NOAA line offices to use when conducting periodic reviews of Active Directory accounts.

Recommendation 3: That the Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator ensure that NOAA's Chief Information Office establish procedures to periodically review Active Directory accounts, passwords, groups, and Group Policy Objects (GPO) for compliance with account management requirements as stated in the Department's policy and following industry best practices. If feasible, utilize specialized Active Directory security tool(s) to conduct periodic reviews.

NOAA Response: We concur. NOAA is working to establish enterprise procedures and to establish a structure under the Continuous Diagnostic and Mitigation (CDM) program to ensure periodic reviews of Active Directory accounts.

Recommendation 4: That the Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator ensure that NOAA's Chief Information Office establish policies or procedures to require compensating controls for service accounts that cannot have regular password changes.

NOAA Response: We concur. NOAA is working to establish enterprise procedures and implement enterprise tools under the Continuous Diagnostic and Mitigation (CDM) program for service accounts that cannot have regular password changes.

Recommendation 5: That the Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator ensure that NOAA's Chief Information Office establish decommission plans with milestones to prioritize and expedite the upgrading or retirement of computers with end-of-life (EOL) operating systems.

NOAA Response: We concur. NOAA is working to establish decommission plans to fully address this recommendation.

011200000388