The National Weather Service Should Further Strengthen Its Protection of Essential Operational Technology

FINAL REPORT NO. OIG-25-012-I

FEBRUARY 27, 2025

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 27, 2025

MEMORANDUM FOR: Vice Admiral Nancy Hann
Deputy Under Secretary for Operations, performing the duties of
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: *The National Weather Service Should Further Strengthen Its Protection of Essential Operational Technology*
Final Report No. OIG-25-012-I

Attached is the final report on our evaluation of the National Weather Service's protection of operational technology. We will post the final report on our website per the Inspector General Act of 1978, as amended (5 U.S.C. §§ 404, 420).

Within 60 calendar days, please provide an action plan addressing the report's recommendations, as required by Department Administrative Order 213-5.

We appreciate your staff's cooperation and professionalism during this evaluation. If you have any questions or concerns about the report, please contact Kevin Ryan, Acting Assistant Inspector General for Audit and Evaluation, at (202) 750-5190 or Chuck Mitchell, Director for Cybersecurity, at (202) 809-9528.

Attachment

cc: Emily Menashes, performing the duties of Assistant Secretary of Commerce for Oceans and Atmosphere and Deputy NOAA Administrator, NOAA
Ken Graham, Director, National Weather Service, NOAA
Ajay Mehta, Acting Director, Office of Planning and Programming for Service Delivery, National Weather Service, NOAA
Zachary Goldstein, Chief Information Officer & Director of High Performance Computing and Communications, NOAA
Beckie Koonge, Assistant Chief Information Officer, National Weather Service, NOAA
Mia Forgy, Director, Audit and Information Management Office, NOAA

Report in Brief

February 27, 2025

Background

Operational technology (OT) consists of programmable systems and devices that directly or indirectly interact with the physical environment. Commonly used OT systems include building badge scanners or temperature sensors for data centers.

Bureaus across the U.S. Department of Commerce (the Department) use OT to support their missions. At the National Weather Service (NWS), within the National Oceanic and Atmospheric Administration (NOAA), deploying OT is critical to providing climate data, forecasts, and warnings to protect people and property and enhance the economy. OT at NWS is spread across the country and ranges from buoys to weather radars. NWS must ensure the availability of these systems by protecting them from cyberattacks.

Implementing zero trust architecture (ZTA) is a critical aspect of protecting OT and defending against increasingly sophisticated and persistent threat campaigns. A key principle of ZTA is distrust of all entities inside and outside the security perimeter. Thus, agencies must secure both OT and the information technology assets that support it against internal and external threats.

The Office of Management and Budget (OMB) instructed federal agencies to meet specific ZTA requirements by the end of fiscal year 2024. These requirements include encrypting internal network traffic and creating reliable asset inventories.

Why We Did This Review

Our objective was to determine whether NWS has implemented effective security controls for its critical OT.

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

The National Weather Service Should Further Strengthen Its Protection of Essential Operational Technology

OIG-25-012-I

WHAT WE FOUND

Overall, we found that NWS has effectively secured its most valuable OT system, System A. However, our review of the three other NWS OT systems identified internal weaknesses related to credential and vulnerability management that could increase the risk of a successful cyberattack. Specifically, we found the following:

I. NWS did not implement strong credential management for some OT systems.

II. NWS lacked complete vulnerability scanning coverage for some OT systems.

NWS should increase the resiliency of its OT systems to defend against the increasing number of cyberattacks that threaten to disrupt its important mission. By implementing our recommendations to improve credential and vulnerability management, NWS will be better prepared to withstand cyberattacks on its OT systems.

WHAT WE RECOMMENDED

We recommended that the Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator ensure the NWS Director implements the following:

1. Review NWS OT systems to ensure that they (a) securely store credentials, including hashes; (b) have debugging disabled where appropriate; and (c) do not use default passwords.

2. Remove insecure protocols such as HTTP and telnet and follow OMB requirements to encrypt internal traffic.

3. Follow the National Institute of Standards and Technology's *Secure Software Development Framework* when developing new systems to ensure that internet access is limited.

4. Conduct vulnerability scanning on all devices within an OT system in accordance with NOAA policy.

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

Operational technology (OT) consists of programmable systems and devices that directly or indirectly interact with the physical environment.[1] Commonly used OT systems include building badge scanners or temperature sensors for data centers.

Cyberattacks against essential OT systems have increased. In November 2023, for example, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) documented attacks on OT used by U.S. water utilities.[2] A May 2024 multiagency report also revealed that pro-Russian hackers were targeting OT systems that support critical infrastructure.[3]

Bureaus across the U.S. Department of Commerce (the Department) use OT to support their missions. At the National Weather Service (NWS), within the National Oceanic and Atmospheric Administration (NOAA), deploying OT is critical to providing climate data, forecasts, and warnings to protect people and property and enhance the economy. OT at NWS is spread across the country and ranges from buoys to weather radars. NWS must ensure the availability of these systems by protecting them from cyberattacks.

Implementing zero trust architecture (ZTA) is a critical aspect of protecting OT and defending against increasingly sophisticated and persistent threat campaigns. The traditional approach to cybersecurity has been to treat internal networks as trusted, meaning that users who have been authenticated are allowed access to everything on the network. However, a key principle of ZTA is that "no actor, system, network, or service operating outside or within the security perimeter is trusted."[4] Thus, agencies must secure both OT and the information technology (IT) assets that support it against internal and external threats.

As part of the federal transition to ZTA, the Office of Management and Budget (OMB) instructed federal agencies to meet specific requirements by the end of fiscal year 2024.[5] These requirements include encrypting internal network traffic and creating reliable asset inventories. The Department and its bureaus are continuing their efforts to fully implement ZTA, which we

---

[1] U.S. Department of Commerce National Institute of Standards and Technology Computer Security Resource Center, September 2023. *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Rev. 3. Washington, DC: DOC NIST CSRC, page 8. Available online at https://csrc.nist.gov/pubs/sp/800/82/r3/final (accessed December 13, 2024).

[2] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, November 28, 2023. *Exploitation of Unitronics PLCs used in Water and Wastewater Systems* [online]. https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems (accessed November 25, 2024).

[3] DHS CISA, May 1, 2024. *Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity* [online]. https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity (accessed October 8, 2024).

[4] Office of Management and Budget, January 26, 2022. *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, OMB M-22-09. Washington, DC: OMB, 2.

[5] Ibid., 1.

recognized as a top management challenge.[6] With an effective ZTA, any potential attackers who gained access to an NWS system would find it difficult to interact with the critical OT that powers the agency.

[6] DOC Office of Inspector General, October 17, 2024. *Top Management and Performance Challenges Facing the Department of Commerce in FY 2025*, OIG-25-001. Washington, DC: DOC OIG. We discussed ZTA implementation in Challenge Area 1: *Modernizing Technology and Systems*.

Objective, Findings, and Recommendations

Our objective was to determine whether NWS has implemented effective security controls for its critical OT. We selected four NWS systems that use OT and examined whether they were adequately protected against cyberattacks. This included evaluating both OT and supporting IT within the systems. Because these are internal NWS systems that contain sensitive information, we refer to them throughout this report by letter: System A, System B, System C, and System D. Appendix A provides a more detailed description of our scope and methodology.

Overall, we found that NWS has effectively secured its most valuable OT system, System A. However, our review of the three other NWS OT systems identified internal weaknesses related to credential and vulnerability management that could increase the risk of a successful cyberattack. Specifically, we found the following:

I. NWS did not implement strong credential management for some OT systems.

II. NWS lacked complete vulnerability scanning coverage for some OT systems.

NWS should increase the resiliency of its OT systems to defend against the increasing number of cyberattacks that threaten to disrupt its important mission. By implementing our recommendations to improve credential and vulnerability management, NWS will be better prepared to withstand cyberattacks on its OT systems.

I. NWS Did Not Implement Strong Credential Management for Some OT Systems

ZTA requires that agencies have a secure internal network. Nation-state threat actors, for example, have consistently demonstrated that they can find ways into seemingly secure networks, as they did with the 2020 cyberattack on the SolarWinds supply chain.[7] As part of our evaluation, we performed technical testing, including an internal penetration test against System B, to determine the impact a cyberattack could have on NWS' network. Our test was a follow-up to previous penetration testing conducted in 2021 and was designed to ensure that NWS remediated past issues.[8] For example, NWS had not effectively secured system credentials, which include usernames and passwords.

We found that although NWS has created a strong network perimeter, it can further improve how it protects credentials on its internal OT systems. Specifically, we identified that NWS (1) did not protect sensitive passwords or password hashes, (2) used a default username and password, (3) used insecure network protocols, and (4) did not adequately secure publicly accessible development websites.

[7] In 2020, the Russian Foreign Intelligence Service compromised U.S. government agencies, critical infrastructure entities, and private-sector organizations by leveraging vulnerabilities in SolarWinds Orion products. *See* DHS CISA, April 15, 2021. *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* [online]. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a (accessed October 8, 2024).

[8] The 2021 penetration test was conducted by an external contractor on behalf of NWS.

A. *NWS did not protect sensitive passwords or password hashes*

Passwords are a traditional way of authenticating a user or service. However, storing or transmitting passwords in plain text, without obscuring the password, presents a security risk. Hashes, which change passwords into a series of letters and numbers, are one way to reduce this risk. For example, using the common Message Digest 5 (MD5) hashing algorithm, a password of "C0mmerce" would correspond to 6c20b8e1e6b7cb9602df224bb42bdc80.

During the 2021 penetration test of System B, testers found plain-text passwords, which allowed them to gain complete control of multiple devices. Although we found that NWS has improved in this area since 2021, we still obtained both plain-text passwords and password hashes for various accounts during our penetration test of System B.

We determined that NWS had misconfigured certain system components. Specifically, an internal website containing several password hashes did not require any authentication to access. The National Institute of Standards and Technology's (NIST's) guidelines state that agencies should store copies of shared or administrator passwords in a secure location.[9] For example, plain-text passwords can be stored in a secure password manager, while password hashes can be stored in a database with proper access controls.

While hashes are generally considered more secure because they cannot be reverted to their original state, anyone with a basic cybersecurity tool can easily crack the hashes for simple passwords such as "C0mmerce."[10] For more complex passwords, attackers with enough time and resources can use brute-force cracking tools to attempt to recover hashed passwords.[11] Regardless, it is important to securely store password hashes to avoid potential cracking attacks.

Additionally, another internal System B website had the debugging function[12] enabled, which we exploited to display a plain-text username and password. Websites with debugging enabled during their development process produce more detailed error messages, which can expose sensitive information not intended for regular users. Therefore, NWS developers should ensure that a website's configuration has debugging disabled before it enters operational use.

---

[9] DOC NIST, *Guide to OT Security*, 107.

[10] The hashed version of a password is not usually accepted through typical authentication operations, such as login prompts. Therefore, an attacker must attempt to "crack" the hash prior to usage.

[11] Brute-force cracking is a technique in which every possible password is generated and compared to the password hash.

[12] A debugging mode or function is specifically designed for testing programming code. It provides additional detailed information about coding errors and should not be deployed with a final software product. *See* The MITRE Corporation. *CWE-489: Active Debug Code* [online]. https://cwe.mitre.org/data/definitions/489.html (accessed November 19, 2024).

If NWS does not properly protect its plain-text passwords as well as password hashes, dedicated attackers—such as those who are state-sponsored—could potentially use them to gain further system access.

B. *NWS used a default username and password*

During our penetration test of System B, we found that an OT component had a default username and password. We accessed the device and discovered that it could send out alert emails to system administrators. An attacker could potentially use this functionality to send phishing emails designed to obtain additional credentials. Emails from internal devices are more likely to be trusted, increasing the likelihood of a successful attack.

NIST states that organizations should "change all default passwords in OT components."[13] This should be done immediately after the component is installed and prior to its deployment. The default username and password for the System B device were in use because they had not been changed following device installation. After we presented our findings to NWS officials, NWS changed the username and password for this OT component. Ultimately, the device remained vulnerable for approximately 6 months.

C. *NWS used insecure network protocols*

Secure network protocols[14] include encryption to ensure that data remains confidential when in transit. We observed that multiple internal websites within System B were using insecure HTTP rather than HTTPS.[15] These included login pages, meaning that users were transmitting their usernames and passwords in plain text. We also noted that some devices allowed telnet connections. Telnet is an insecure legacy protocol used to remotely control a device. Like HTTP, telnet transmits credentials in plain text.

As part of the shift to ZTA, OMB requires agencies to remove insecure protocols from their networks. Specifically, OMB has stated that agencies must encrypt all internal network traffic and required them to remove HTTP by the end of fiscal year 2024.[16] Additionally, Department policy requires that bureaus encrypt remote connections, which prohibits the use of telnet.

When we presented the results of our testing, NWS officials were unaware that telnet was enabled for two devices on System B. Following our briefing, NWS disabled telnet on these devices.

Although NWS was aware of the HTTP issue, it had not yet fully implemented OMB's requirements to replace it with HTTPS. While newly created websites are deployed

[13] DOC NIST CSRC, *Guide to OT Security*, 107.

[14] A network protocol is a communication standard that defines how devices exchange data.

[15] "HTTP stands for Hypertext Transfer Protocol, and is the primary protocol used to serve web content, as well as other internet data." *See* OMB M-22-09. Encrypted HTTP traffic is easy to identify because the website has an "s" after "http" (for example, https://www.oig.doc.gov/).

[16] OMB, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, 3-4.

using HTTPS, NWS stated that it will address legacy HTTP websites as part of a modernization project in fiscal year 2026.

HTTPS is a core piece of ZTA. Until NWS updates its legacy websites, it will be unable to fully implement ZTA. If an attacker were to gain access to NWS networks, they could potentially intercept credentials sent with insecure protocols and use those credentials to gain additional access.

D. NWS did not adequately secure publicly accessible development websites

NWS is in the process of migrating System C to a modern platform. In addition to ensuring the system remains viable well into the future, the new system is intended to meet modern security requirements. For example, the current System C relies on legacy technology and cannot securely store and transmit credentials. The new system is designed to fully support encryption.

As part of the development of this new system, NWS created publicly accessible websites. NWS reported that the development websites had been set up to facilitate system testing across multiple regions. While each was protected by a username and password, anyone could visit the websites via the public internet. The connection to the websites was also via HTTP rather than HTTPS, meaning that users sent their login credentials unencrypted over the internet.

We reviewed one of the System C development websites and found that it primarily contained test data. However, upon further inspection, we discovered plain-text usernames and passwords within the comments of old configuration files. Both the usernames and passwords were short and could have been easily guessed. Considering their simplicity, it is possible that an attacker could have gained access to the development website. While that attacker would have been unable to affect current NWS operations, they could potentially have gathered information that could be useful in a future attack on the completed system.

Further, we found that internet scanning tools had detected the System C development websites, meaning that any member of the public could locate them. The development websites also contained a standard banner[17] that identified them as U.S. government systems, which could have invited additional attention from attackers. NIST's *Secure Software Development Framework* recommends that organizations minimize internet access to only what is necessary.[18]

---

[17] A message that informs users of the implications of accessing a computer resource (such as consent to monitor). *See* Committee on National Security Systems, March 2, 2022. *Committee on National Security Systems (CNSS) Glossary*, CNSSI No. 4009. Fort George G. Meade, MD: CNSS, 177. Available online at https://www.cnss.gov/CNSS/issuances/Instructions.cfm (accessed November 19, 2024).

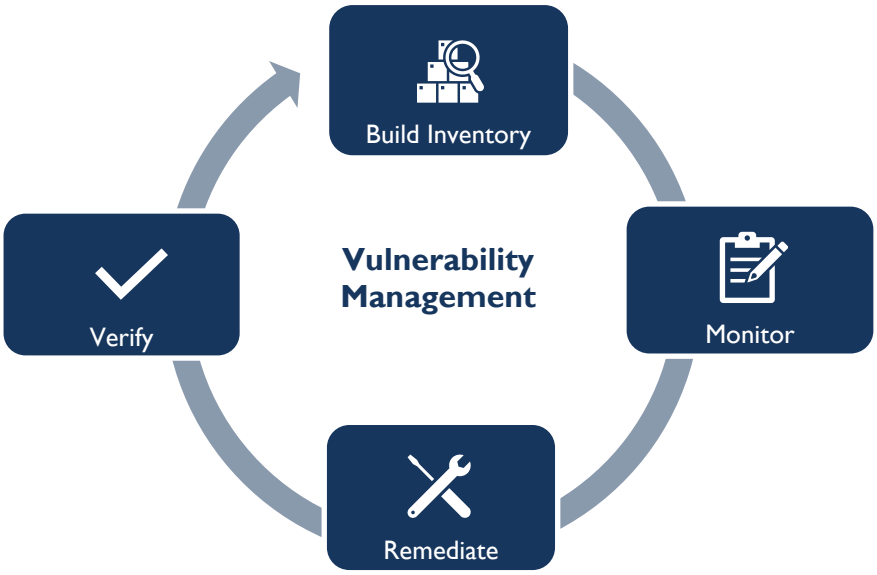
[18] DOC NIST CSRC, February 2022. *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*, NIST SP 800-218. Washington, DC: DOC NIST CSRC, 8. Available online at https://csrc.nist.gov/pubs/sp/800/218/final (accessed October 4, 2024).

Ultimately, NWS did not implement simple controls such as using HTTPS or limiting access to those users already authenticated on the NWS network. After we completed our review, NWS removed the development websites from the internet.

II. NWS Lacked Complete Vulnerability Scanning Coverage for Some OT Systems

During a cyberattack, hackers can exploit a vulnerability on a single device and use it as a foothold into the network. The goal of vulnerability management is to identify and remediate device vulnerabilities, reducing the number of potential compromise points in a network. The Department has developed a vulnerability management policy that incorporates various federal mandates into a central document. This policy requires that bureaus implement the four phases of the vulnerability management lifecycle, as shown in figure 1.[19]

Figure 1. Vulnerability Management Lifecycle



Source: Adapted from Department guidance

To implement the Monitor stage, NOAA requires that all its internal devices be scanned weekly. However, during our penetration test of System B, we found that some devices were not receiving the required vulnerability scans. In one instance, an unscanned device had reached its end of life[20] and presented a security risk. CISA warns that end-of-life software poses a consequential risk to systems and recommends the retirement of all end-of-life products.

[19] DOC, February 2024. *Vulnerability Management Standard* (internal Department document).

[20] *End of life* means the vendor no longer provides security or maintenance for the product. Under these conditions, the device would be vulnerable to any newly discovered exploits.

We found that NWS had not configured its device discovery tools to scan the full network of System B devices. This left some devices out of System B's inventory and prevented NWS from having an accurate picture of the risk the system faced. As noted in Figure 1, the first step of the vulnerability management lifecycle is to build an inventory. A complete inventory ensures that all devices in a system are included in the Monitor stage and receive vulnerability scans.

After we informed NWS system administrators of our findings, they updated the configuration of their device discovery tools to include 4 additional subnets[21] and removed the end-of-life device.

We also observed a similar issue on System D, which was not receiving regular vulnerability scans. Approximately 90 percent of system devices were not receiving the required weekly scans. In this case, NWS was aware of the issue and reported that it lacked a centralized method to conduct vulnerability scanning. The system's devices are located across the United States. As a result, multiple offices have been responsible for scanning the devices.

To remediate this issue, NWS has launched a project to centralize the scanning and management of System D devices. The project's completion, scheduled for June 2025, is intended to enable NWS to perform consistent vulnerability scans on all devices within the system. NWS has made progress by installing a centralized scanning tool. However, until the project is complete, NWS will lack insight into potential vulnerabilities in this system—which may allow an attacker to exploit them.

Conclusion

Throughout our evaluation, we noted that NWS has developed a strong network perimeter, which is a good first line of defense against cyberattacks. However, due to increasingly sophisticated threat actors and as part of the shift to ZTA, NWS must maintain strong internal security as well. This is especially important for OT systems, which interface with the physical world. By improving its credential and vulnerability management, NWS can increase the resiliency of its OT systems against cyberattacks that could disrupt its critical mission.

Recommendations

We recommend that the Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator ensure the NWS Director implements the following:

1. Review NWS OT systems to ensure that they (a) securely store credentials, including hashes; (b) have debugging disabled where appropriate; and (c) do not use default passwords.
2. Remove insecure protocols such as HTTP and telnet and follow OMB requirements to encrypt internal traffic.

[21] A subnet, or subnetwork, is a physically or logically segmented section of a larger network.

3. Follow NIST's *Secure Software Development Framework* when developing new systems to ensure that internet access is limited.
4. Conduct vulnerability scanning on all devices within an OT system in accordance with NOAA policy.

Summary of Agency Response

On February 14, 2025, we received NOAA's formal response to our draft report. NOAA concurred with our findings and recommendations and described actions it has taken, or will take, to address them. NOAA's formal response is included within this final report as appendix B.

We are pleased that NOAA concurred with our recommendations and look forward to reviewing its proposed action plan.

Appendix A: Objective, Scope, and Methodology

Our objective was to determine whether NWS has implemented effective security controls for its critical OT. To accomplish our objective, we judgmentally selected four NWS systems that use OT and performed the following actions:

- Interviewed system administrators and bureau management.
- Reviewed prior penetration test results from external NWS contractors and other federal agencies.
- Examined NWS system configurations for development and production OT systems.
- Performed an internal penetration test against one NWS system.

We reviewed each of the selected systems' compliance with the following applicable internal controls, provisions of law, and mandatory guidance:

- Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283
- OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, dated January 2022
- NIST Special Publications:
    - 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020
    - 800-82, Revision 3, *Guide to Operational Technology Security*, dated September 2023
    - 800-207, *Zero Trust Architecture*, dated August 2020
    - 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*, dated February 2022
- Department *Enterprise Cybersecurity Policy*, dated September 2022
- Department *Vulnerability Management Standard*, dated February 2024
- NOAA *IT Security Manual (ITSM)*, version 8.0, dated September 2023
- NOAA *Security and Privacy Control Matrix (SPCM)*, version 8.0

We did not rely on computer-processed data to support our findings, conclusions, or recommendations. We omitted certain technical information in the report for security reasons.

We conducted our evaluation from March 2024 through February 2025 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401-424), and Department

Organization Order 10-13, as amended October 21, 2020. We performed our work remotely as well as at NWS locations in Silver Spring, MD, and Sterling, VA.

We conducted this evaluation in accordance with Quality Standards for Inspection and Evaluation (December 2020) issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that the evidence must sufficiently and appropriately support evaluation findings and provide a reasonable basis for conclusions and recommendations related to the objective. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our review objective.

Appendix B: Agency Response

NOAA's response to our draft report begins on the following page.

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

MEMORANDUM FOR: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation
U.S. Department of Commerce
Office of Inspector General

FROM: VADM Nancy Hann
Nancy Hann, VADM/NOAA
Deputy Under Secretary for Operations
Performing the duties of Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator

SUBJECT: *The National Weather Service Should Further Strengthen Its Protection of Essential Operational Technology*
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 the Evaluation of the National Weather Service's Protection of Operational Technology. We reviewed the report and concurred with the recommendations.

We appreciate the opportunity to review and respond to your draft report. If you have questions, please contact Mia Forgy, Director, Audit and Information Management Office on (301) 427-7893.

Attachment

Department of Commerce
National Oceanic and Atmospheric Administration
Response to the OIG Draft Report Entitled
The National Weather Service Should Further Strengthen Its Protection of Essential Operational Technology
(January 2025)

General Comments

The National Oceanic and Atmospheric Administration (NOAA), National Weather Service (NWS) appreciates the opportunity to review the Office of Inspector General's (OIG) draft report on Evaluation of the National Weather Service's Protection of Operational Technology (OT). NOAA reviewed the draft report and concurs with the OIG's recommendations. General comments and responses to the four recommendations are provided below.

NOAA Response to OIG Recommendations

Recommendation 1: Review NWS OT systems to ensure that they (a) securely store credentials, including hashes; (b) have debugging disabled where appropriate; and (c) do not use default passwords.

NOAA Response: We concur. The OT system's Federal Information Security Management Act (FISMA) personnel have opened two (2) plans of actions and milestones (POA&Ms) to mitigate Recommendation 1 (a) and (c). Additionally, the mitigations to address Recommendation 1 (b) were applied in July 2024, upon initial identification by the OIG team.

Recommendation 2: Remove insecure protocols such as HTTP and telnet and follow OMB requirements to encrypt internal traffic.

NOAA Response: We concur. NWS staff took-action in September 2024 to disable Telnet on system B once it was identified as present. System B's IT Modernization project (continues through FY 2026) will continue to ensure we address internal sites using Hypertext Transfer Protocol (HTTP) by either a) migrating the site to HTTPS or b) decommissioning the site, following OMB requirements to encrypt internal traffic.

Recommendation 3: Follow NIST's Secure Software Development Framework when developing new systems to ensure that internet access is limited.

NOAA Response: We concur. Immediate actions were taken to close this vulnerability in June 2024 upon identification by the OIG team.

Recommendation 4: Conduct vulnerability scanning on all devices within an OT system in accordance with NOAA policy.

NOAA Response: We concur. System B addressed the vulnerability scanning deficiency immediately upon identification by the OIG team in July 2024 with validation of 100 percent coverage during annual continuous monitoring assessment and authorization (A&A) activities in November 2024. System D has opened a POA&M to address the vulnerability scanning

deficiencies. Additionally, the system has deployed NOAA's Big Fix System (NBFS) to mitigate residual risks of operation.

Recommended Changes for Factual/Technical Information

None

Editorial Comments

None