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.