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.