Report in Brief

August 27, 2024

Background

The National Oceanic and Atmospheric Administration's (NOAA's) National Environmental Satellite, Data, and Information Service (NESDIS) provides access to global environmental data from satellites and other sources. Current NESDIS ground systems process data from NOAA and non-NOAA satellites and other observing systems.

NESDIS is transitioning some functionality from its current satellite ground systems to its cloud-based NESDIS Common Cloud Framework (NCCF). The NCCF is intended to provide greater flexibility, efficiency, cybersecurity, and cost effectiveness for the next generation of NESDIS missions.

Unlike NESDIS' prior ground systems, the responsibility for implementation of the NCCF does not fall under any single satellite program. It is being led by a separate NESDIS office, the Office of Common Services (OCS).

Why We Did This Audit

Our audit objective was to assess NESDIS' progress implementing the NCCF. We examined aspects of the management and execution of the NCCF effort as well as the extent to which existing security controls adequately protected the system from cybersecurity threats.

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

A Lack of Program Management Controls and Attention to IT Security Threatens the Success of NOAA's Effort to Implement a Cloud-Based Common Ground System

OIG-24-034-A

WHAT WE FOUND

We found that (1) NESDIS' effort to implement the NCCF lacks fundamental project management practices set forth in Department of Commerce policy, (2) NOAA is not reporting the NCCF's financial, project, and performance data to the federal IT dashboard, (3) NESDIS' penetration testing of the NCCF has been inadequate, and (4) the NCCF is built on a cloud platform that cannot support its security requirements.

WHAT WE RECOMMEND

We recommend that the NOAA Administrator direct the NOAA Deputy Undersecretary of Operations to ensure NESDIS:

1. Identifies the NCCF effort as a program or project in accordance with DAO 208-16.
2. Implements appropriate, formal management controls for the NCCF.
3. Delivers official requirements to OCS for development of the NCCF.
4. Directs OCS to comply with all aspects of NESDIS requirements management policy.

We recommend that the NOAA Administrator direct the NOAA Deputy Undersecretary of Operations to:

5. Ensure NCCF financial, project, and performance data is reported to OMB via the Federal IT Dashboard, in accordance with federal budget guidance.

We recommend that the NOAA Administrator direct the NOAA Deputy Undersecretary of Operations to ensure NESDIS:

6. Updates the NESDIS penetration testing process to ensure: (a) penetration testers have adequate access to examine all system components, (b) penetration test findings are documented in Plans of Action and Milestones (POA&Ms) in the security system of record, (c) penetration tests are conducted prior to the creation of the Security Assessment Report (SAR) that supports the annual authorization process, and (d) the SAR includes penetration test results and any testing limitations that testers encountered.
7. Includes root cause analysis and closure as part of the POA&M process.
8. Conducts an after-action review to determine the root cause(s) of the security weaknesses detailed in the OIG penetration test report and creates POA&M(s) to resolve the root cause(s).
9. Migrates the NCCF cloud system to a FedRAMP® approved high-impact cloud platform or provides the equivalent protection.
10. Revises NCCF security documents to ensure security controls align with the high-impact security requirements.
11. Updates the NCCF's analysis of alternatives to include moving to a multi-region architecture and document a risk and cost-based decision on how NESDIS will meet the NCCF's availability requirements.