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

FINAL REPORT NO. OIG-24-034-A

AUGUST 27, 2024

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

August 27, 2024

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: *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*
Final Report No. OIG-24-034-A

Attached is our final report on the audit of the National Oceanic and Atmospheric Administration's (NOAA's) implementation of a cloud-based common ground system. Our audit objective was to assess the National Environmental Satellite, Data, and Information Service's (NESDIS') progress implementing the NESDIS Common Cloud Framework (NCCF).

We found the following:

I. NESDIS' effort to implement the NCCF lacks fundamental project management practices, which must be addressed to ensure long-term success.

II. NOAA is not reporting the NCCF's financial, project, and performance data to the Federal IT Dashboard, reducing project oversight and accountability.

III. NESDIS' penetration testing of the NCCF has been inadequate, leaving it vulnerable to cyberattack.

IV. The NCCF is built on a cloud platform that cannot support its security requirements, putting critical data at risk.

In its response to our draft report, NOAA concurred with all recommendations and described actions it has taken, or will take, to address them. NOAA's response is included in appendix C.

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 the Inspector General Act of 1978, as amended (5 U.S.C. §§ 404 & 420).

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; Kevin Ryan, Director for Audit and Evaluation, Systems Analysis and NOAA Programs, at (202) 750-5190; or Edward Kell, Director for Audit and Evaluation, Satellite Programs, at (202) 753-6125.

Attachment

cc: Jainey K. Bavishi, Assistant Secretary of Commerce for Oceans and Atmosphere and Deputy NOAA Administrator
Vice Admiral (Select) Nancy Hann, Deputy Under Secretary for Operations, NOAA
Karen Hyun, Chief of Staff, NOAA
Stephen Volz, Assistant Administrator for Satellite and Information Services, NOAA
Heather Kilcoyne, Director, Office of Common Services, NOAA

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.

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.

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.[1] This data is used to promote and protect the nation's security, environment, economy, and quality of life. Current NESDIS ground systems control satellites and ingest, process, store, and distribute environmental data and products. The computing architecture for many of NESDIS' ground systems is currently located "on premises" rather than in the cloud and was developed with unique designs specific to each mission.

NESDIS' ground systems support two Primary Mission Essential Functions (PMEF) for the Department of Commerce and multiple strategic objectives at both the Department and NOAA levels.[2] Additionally, due to the criticality of NESDIS' mission, its ground systems are categorized as high impact, which describes the potential effects of a security breach.[3] NESDIS' ground systems must be highly available and maintain a high degree of data integrity to support emergency response and ensure users can rely on the resulting products and services NOAA provides.

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; see figure 1). The NCCF is intended to provide NESDIS with:

- *Secure ingest* of NOAA and partner data, including scalability to accommodate an increase in future data sets and built-in screening for security threats
- *Data processing and product generation* on a high-performance computing architecture that is scalable to future needs
- *Data dissemination* to users via a single portal
- *Data archive and storage* that combine NOAA and partner data in a common, accessible location, enabling innovations like artificial intelligence
- *A science sandbox* where scientists and developers can investigate new uses for NESDIS' environmental data and perform research

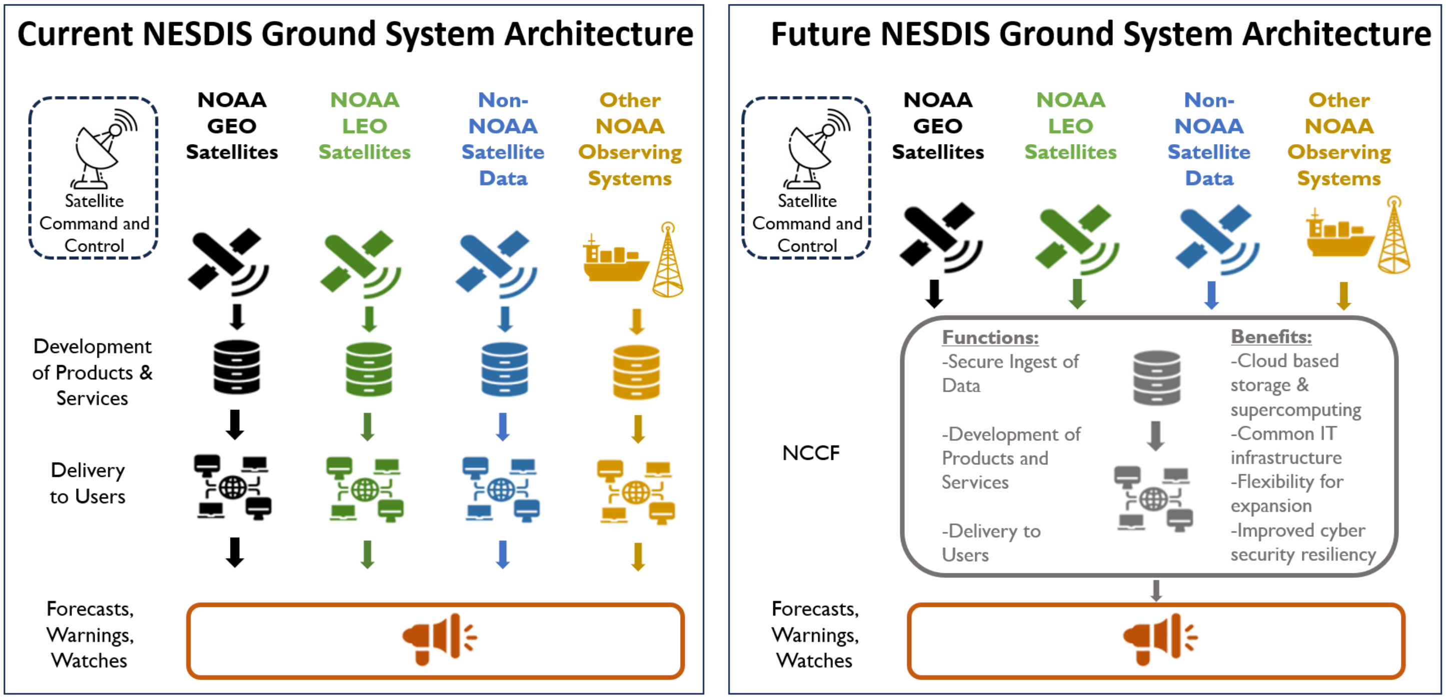
Satellite command and control, used for NOAA satellites' on-orbit operations—including maintenance of electronics, instrument calibrations, and orbital positioning adjustments—is not part of the NCCF and will remain with the individual satellite ground systems.

[1] NESDIS currently owns and operates four geostationary satellites (GEO), five polar-orbiting satellites (LEO), and one deep space satellite. It also receives data from government partners and commercial providers.

[2] NESDIS ground systems support Department of Commerce PMEF No. 2: Provide Satellite Imagery and PMEF No. 3: Provide Meteorological Forecasts.

[3] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) 199, February 2004, *Standards for Security Categorization of Federal Information and Information Systems,* defines three levels (low, moderate, and high) of potential impact on organizations or individuals should there be a breach of security. High impact means that the "loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals."

Figure 1. Current and Future NESDIS Ground System Architecture


Current NESDIS Ground System Architecture
Satellite Command and Control
NOAA GEO Satellites
NOAA LEO Satellites
Non-NOAA Satellite Data
Other NOAA Observing Systems
Development of Products & Services
Delivery to Users
Forecasts, Warnings, Watches
Future NESDIS Ground System Architecture
Satellite Command and Control
NOAA GEO Satellites
NOAA LEO Satellites
Non-NOAA Satellite Data
Other NOAA Observing Systems
NCCF
Functions:
-Secure Ingest of Data
-Development of Products and Services
-Delivery to Users
Benefits:
-Cloud based storage & supercomputing
-Common IT infrastructure
-Flexibility for expansion
-Improved cyber security resiliency
Forecasts, Warnings, Watches

Source: Office of Inspector General (OIG) derived from NESDIS ground system documentation

The transition to the NCCF supports Department-level strategic objectives to enhance observational infrastructure and modernize mission support processes by eliminating duplication and operational inefficiencies. The NCCF is intended to provide greater flexibility, efficiency, cybersecurity, and cost effectiveness as NESDIS prepares for its next generation of missions and maintains the operations of current satellite missions.[4] 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).

The NCCF is intended to provide flexibility, efficiency, cybersecurity, and cost effectiveness for the next generation of NESDIS missions.

[4] In the future, NESDIS will add the Geostationary Extended Observations, Near Earth Orbit Network, and Space Weather Follow-On programs and associated satellite missions to its current portfolio of satellites.

Objective, Findings, and Recommendations

Our audit objective was to assess NESDIS' progress implementing the NCCF. To satisfy our objective, 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. See appendix A for a full description of our scope and methodology.

We found that (1) NESDIS' effort to implement the NCCF lacks fundamental project management practices set forth in Department of Commerce policy, which must be addressed to ensure long-term success, (2) NOAA is not reporting the NCCF's financial, project, and performance data to the Federal IT Dashboard, reducing project oversight and accountability, (3) NESDIS' penetration testing of the NCCF has been inadequate, leaving it vulnerable to cyberattack, and (4) the NCCF is built on a cloud platform that cannot support its security requirements, putting critical data at risk.

Remediating these deficiencies is important to ensure the NCCF is successfully implemented, accountable to oversight, and operationally secure. In particular, without program or project management controls to measure and monitor its cost and technical performance, the NCCF effort lacks sufficient accountability. The absence of formal requirements management processes leaves the effort at risk of not meeting NESDIS' goals for the system. The lack of reporting NCCF data to the Federal IT Dashboard removes it from the review of oversight entities that enable accountability to the American people. Finally, NESDIS cybersecurity assessment deficiencies, security weaknesses, and architecture issues leave the system vulnerable to attack and regional outages. NOAA must address these issues to ensure that the goals for the NCCF—to provide greater flexibility, efficiency, cybersecurity, and cost effectiveness—are met.

I. NESDIS' Effort to Implement the NCCF Lacks Fundamental Project Management Practices, Which Must Be Addressed to Ensure Long-Term Success

NESDIS' effort to implement the NCCF is significant to NOAA achieving its mission, but NESDIS has neither established appropriate cost and performance management controls nor provided official requirements to OCS.

A. The NCCF effort lacks management controls needed to measure cost and technical performance

NOAA guidance defines a *project* as any undertaking to create a service, product, system, and/or system upgrade in support of a validated NOAA mission requirement.[5] The Department further designates certain projects as "high profile" based on various factors, including (1) projects that are key to the Department's mission goals and

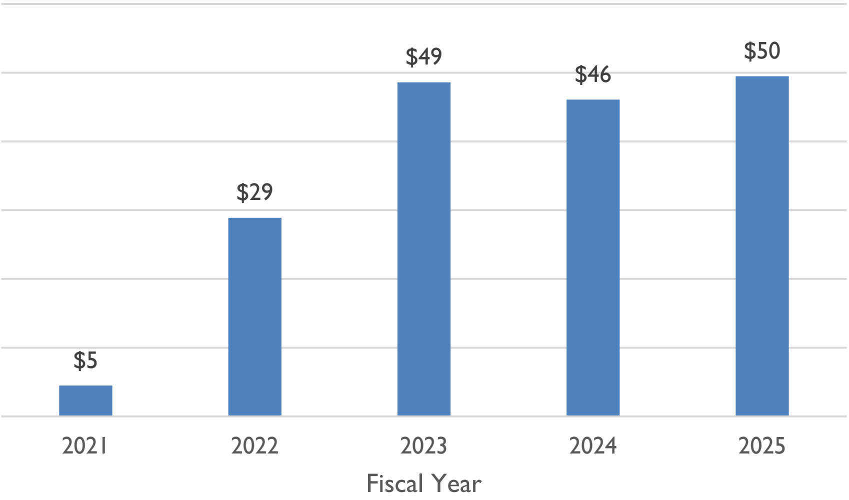
[5] NOAA Administrative Order 206-108, October 2005. *Requirements Management*, section 6.10.

objectives[6] and (2) IT projects having lifecycle costs[7] of more than $75 million or annual costs exceeding $30 million.[8] Department project management policy[9] states that high-profile projects are required to have schedules, cost estimates, reviews by independent boards at major milestones in the project's life, and performance baselines.[10]

The NCCF is of sufficient importance that the Department now considers it a high value asset (HVA).[11] The Department of Homeland Security further designated the NCCF as a Tier 1 HVA, meaning it is critical to the agency and the nation. NESDIS also reports the status of the NCCF to the NOAA Program Management Council (PMC), which oversees mission-critical and large-scale projects within NOAA.

In addition, NCCF spending (see figure 2) through fiscal year (FY) 2023 of approximately $82 million already exceeds Department lifecycle cost spending thresholds for high-profile IT projects. Single year spending rates from FY 2023 through FY 2025 also exceed thresholds, and similar rates of spending are expected to continue through FY 2027.

Figure 2. NCCF Spending in Millions, Actual (FYs 2021–2023) and Projected (FYs 2024 and 2025)



Source: OCS-provided financial data, rounded to the nearest million dollars

[6] Department Administrative Order (DAO) 208-16, May 2015. *Acquisition Project Management*, section 3.05.a.1.
[7] According to the Department's acquisition management guidance, lifecycle cost includes the cost of design, development, verification, production, operation, maintenance, support, and retirement of a program or project over its planned lifespan.
[8] DAO 208-16, section 3.05.b.2.
[9] DAO 208-16, sections 4.02 and 4.03.
[10] A baseline is a cost, schedule, and performance goal that will be the standard against which actual work is measured. NESDIS guidance further describes a cost baseline as how much cost the project is expected to incur against specific work, which is driven by the project's defined requirements (NESDIS Handbook 1224.1, December 2020. *NESDIS Project Cost and Schedule Status Tracking Handbook*).
[11] According to the Department's HVA handbook, an HVA is "information or an information system with informational value, that is mission essential, or that is designated as Federal Civilian Enterprise Essential (FCEE), the compromise of confidentiality, integrity, or availability of which would have a serious impact to the Department and the Federal Government."

Despite the NCCF effort's significance and size, NESDIS has not formally established it as a project or a program,[12] and several fundamental management controls are missing. The NCCF effort does not have cost or technical baselines; these are standard tools for measuring project health and progress. NESDIS also does not have a lifecycle cost estimate for the NCCF, which according to the Department's guidance, is needed to assess affordability and the impact of changes and to maintain an appropriate level of project control.[13]

The NCCF effort lacks several fundamental management controls.

In FY 2021, OCS began work on the NCCF as a level of effort pilot activity, and because of this classification NESDIS did not establish typical program or project management controls.[14] The NCCF team successfully delivered the cloud infrastructure in FY 2021 with further refinement in FY 2022 and, as a result, the effort's funding grew from $5 million in FY 2021 to $49 million in FY 2023. However, NESDIS did not implement management controls associated with what is now a larger, more important IT acquisition and development program or project, even though it is beyond the point at which it can appropriately be designated as a pilot.

Thus, NESDIS does not have the management controls needed to monitor and measure cost and technical performance for the NCCF. Without these controls, NESDIS lacks mechanisms to ensure accountability and long-term success for the effort.

B. *The NCCF effort lacks a requirements management board, a requirements management plan, and official requirements*

NESDIS policy describes requirements management as a process used to gather, analyze, decompose, validate, track, and manage changes to requirements.[15] This policy requires NESDIS to deliver official requirements to its offices, in this case OCS, to define what is expected of the activities it manages.[16] The requirements from NESDIS should be the starting point from which OCS derives more detailed functional requirements to guide the development of the NCCF.

NESDIS policy also requires OCS to have its own requirements management board that documents the procedures and obtains the resources to implement the requirements management processes for projects within OCS.[17] The board would ensure NESDIS has issued official requirements to OCS for the NCCF. It would also author a requirements

[12] Pursuant to Department policy DAO 208-16, a "project" is a collection of discrete activities, acting as a system, with specific output that achieve a clearly defined objective and support an overall program goal. A "program" is a consolidated effort to achieve a defined goal and includes a collection of ongoing activities, as well as finite projects, with objectives that achieve a specific purpose or outcome of a departmental strategic goal or as required by statute or regulation.

[13] *DOC Acquisition Agile Program and Project Management Guidebook,* version 1.0, December 2023, p. 43.

[14] DAO 208-16 defines a "level of effort activity" as a funded activity that does not meet the definition of a program or project.

[15] NESDIS Procedural Requirement 1302.1, March 2019. *Requirements Management,* section P.1.

[16] *Ibid.,* section 3.1.d.

[17] *Ibid.*, sections 3.2.2 and 3.3.1.

management plan to provide specific guidance on how the requirements management process is executed for the NCCF.

However, NESDIS has not issued official requirements for the development of the NCCF as it would if it was designated as a program or project. In addition, OCS does not have a requirements management board or a requirements management plan for the NCCF.

In the absence of official NESDIS requirements, OCS personnel took steps to create NCCF requirements from other sources. OCS derived top-level system requirements from a 2021 NESDIS memo authorizing the development and migration of mission capabilities to the NCCF. OCS then created lower-level requirements from these "memo-driven" requirements to develop the NCCF.

As described previously, NESDIS began the NCCF effort as a small level of effort pilot activity, in which the effort would only move forward after clearly demonstrating new capability. The 2021 authorization memo was enough direction for OCS to start working toward demonstration of the NCCF's initial capabilities. However, as also described previously, the NCCF effort has now grown to the scale of a program or project and should be managed accordingly.

Without official NESDIS requirements, a requirements management board, and a requirements management plan, OSC does not have a means to (1) know if it has gathered the correct requirements to meet NESDIS' expectations for its new enterprise data management solution, (2) verify completion of those requirements, (3) validate that the NCCF, "as built," will meet NESDIS' intent for its new enterprise data management solution, and (4) ensure ongoing consistency between NESDIS' needs and the design of the NCCF.

Conclusion

NESDIS will enable better oversight and management control and ensure the long-term success of its NCCF effort by establishing it as a program or project with cost, schedule, and technical baselines, delivering official requirements to OCS that align with NESDIS' expectations for the NCCF, and managing those requirements according to its policy. These actions would put planned funds for the NCCF to better use by ensuring efficient and effective progress to deliver a system that aligns with user needs.

Recommendations

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 as described in the *DOC Acquisition Agile Program and Project Management Guidebook,* including a formal lifecycle cost estimate; cost, schedule, and technical performance baselines; and performance measurement against those baselines.
3. Delivers official requirements to OCS for development of the NCCF.
4. Directs OCS to comply with all aspects of NESDIS requirements management policy, including establishment of a requirements management board to oversee requirements and creation of a requirements management plan for the NCCF.

Implementing these four recommendations will put planned funds for the NCCF to better use.[18]

II. NOAA Is Not Reporting the NCCF's Financial, Project, and Performance Data to the Federal IT Dashboard, Reducing Project Oversight and Accountability

Federal budget guidance from the Office of Management and Budget (OMB)[19] requires agencies to regularly submit their IT financial, project, and performance data to the Federal IT Dashboard.[20] Major IT investments require the highest level of reporting detail, including a business case that describes project planning, performance, and risks in an effort to ensure the investment continues to add sufficient value to the agency.

Major IT investments are defined in federal budget guidance as those (1) involving Tier 1 HVAs, (2) that are important to the agency's mission and require special management attention, (3) with high visibility to Congress or the public, and (4) with high annual or lifecycle costs. Additionally, the Department has reinforced the federal requirements by issuing its own supplemental guidance stating that major IT investments must report detailed cost and schedule performance data against established baselines to OMB.

The NCCF is a major IT investment: it is a Tier 1 HVA, is important to the agency's mission, and has high annual and total costs (see finding I.A). However, NOAA does not report NCCF financial, project, and performance data to the Federal IT Dashboard as required by both federal and Department guidance.

[18] We identified $98 million of projected NCCF funding in FY 2025 and FY 2026 that would be put to better use (see appendix B for identification of potential monetary benefits).
[19] OMB Circular A-11, August 2023. *Preparation, Submission, and Execution of the Budget*, section 55.3.
[20] The Federal IT Dashboard, itdashboard.gov, enables the public, agencies, Congress, and other oversight organizations to understand the status and impact of federal IT investments. OMB Circular A-11 states that updates to the Federal IT Dashboard should be made "as necessary" to reflect the most current information for reported projects.

In 2012, a combined NOAA and NESDIS independent review team study found that Department and NOAA oversight of major satellite programs at the time should be streamlined—it concluded that there were too many parties in the reporting chain and confusion about who was responsible for success of the satellite programs. The Department took subsequent action and reached an agreement with NOAA. In particular, in 2013, the NESDIS Assistant Chief Information Officer notified NESDIS leadership of the agreement to remove seven satellite ground systems "being acquired under specific satellite acquisition efforts and current operational ground systems" from OMB IT reporting requirements. The intent of this agreement was to enable more focused, efficient information flow and decision making and align with how other agencies (including NASA) were reporting their satellite investments.

The Assistant Chief Information Officer's 2013 email stated that final OMB approval of this path was pending, but NESDIS was not able to provide us with evidence of OMB's 2013 approval. The NCCF is not listed in the agreement (the NCCF did not exist in 2013), but NOAA stated that the 2013 agreement applies to the NCCF because most of its current functionality is related to processing satellite data. NOAA has not discussed the applicability of the 2013 agreement to the NCCF with OMB.

Notwithstanding NOAA's position, the NCCF effort does not fall within the 2013 agreement. First, it is not being acquired under any specific satellite system acquisition effort. Instead, the NCCF is a major IT investment being run by OCS, an office that is separate from the satellite program offices, without the oversight mechanisms of NOAA's traditional satellite programs. In addition, the NCCF's planned capabilities for storage, archive, distribution, and the new science sandbox exceed those of traditional satellite ground systems.

NOAA's current lack of reporting of NCCF data removes the project from even the possibility of OMB review. OMB, however, is required to oversee IT budgeting and evaluate the risks of all major IT investments. It seeks to improve agencies' use of IT and enhance the effectiveness, efficiency, and productivity of government operations. Additionally, the Government Accountability Office (GAO) has reported on the status of and issues with cloud computing projects in the federal government—many of its reports rely on source data from the Federal IT Dashboard.[21] NOAA has recognized that a small portion of the NCCF system—including its storage, archiving, and science sandbox features—should be reported and is planning to track and report those areas separately. However, this approach would exclude most of the NCCF (a major IT system) from this oversight.

Recommendation

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.

[21] For example, see GAO-23-105482, May 2023, *Cloud Security: Selected Agencies Need to Fully Implement Key Practices*.

III. NESDIS' Penetration Testing of the NCCF Has Been Inadequate, Leaving It Vulnerable to Cyberattack

The NCCF's past penetration tests were either incomplete or inadequately documented, leading to a failure to address persistent issues. We performed our own penetration testing on the system and were able to gain complete control of the NCCF using only basic cyberattacks, indicating that NOAA's environmental data was not secure.

A. Prior penetration tests were incomplete, results were not properly documented, and NESDIS did not effectively resolve the security issues that were discovered

The NCCF undergoes an annual security authorization process to assess its security posture and formally approve its authority to operate. Because the NCCF is a high-impact system, its annual security authorization process requires penetration testing. According to the NCCF's security policy, all system components must be included in this testing.

Upon completion of penetration testing, NCCF personnel must document the results in Plans of Action and Milestones (POA&Ms) in the Department's system of record to track and correct any issues.[22] Any identified vulnerabilities should then be included in annual Security Assessment Reports (SARs).[23] During the NCCF's annual security authorization process, NOAA authorizing officials review its SAR, which should include the penetration testing results and the validation of completed POA&Ms to inform the authorization to operate decision.

Our own penetration testing of the NCCF found several issues that had also been identified during previous tests, indicating that the issues had not been addressed. This led us to further review the NCCF's penetration testing process to understand why.

We found that while NESDIS conducted annual penetration tests on the NCCF in October 2022 and August 2023, neither test reviewed all system components, due to access issues with the credentials issued to testers. Yet even without reviewing all system components, penetration testers identified vulnerabilities that they recommended be corrected immediately due to the imminent likelihood of exploitation. These issues were not documented as POA&Ms in the Department's cybersecurity system of record; instead, NCCF personnel used internal tracking software. Further, the discrete system vulnerabilities tracked in the internal software were closed when developers corrected them without sufficient scrutiny into whether the root cause was addressed.[24] With no POA&Ms in the system of record, and discrete system

[22] A POA&M is a document that outlines the specific steps, or actions, that an organization intends to take to remediate vulnerabilities identified during a security assessment or audit. It serves as a roadmap for managing risk, detailing the milestones for addressing each identified issue, including responsible parties, resources required, and target completion dates.

[23] SARs document the findings and conclusions derived from evaluating the security posture of an information system or organization against various threats and vulnerabilities. They are used during annual authorization decisions to inform the authorizing official(s).

[24] As a result, our penetration testing identified more instances of the same vulnerabilities.

vulnerabilities closed in the internal tracking system, the findings were not included in the corresponding SARs as required.

However, we also found that the NCCF's 2022 penetration testing took place in October, well after the August publication of the SAR and the completion of the NCCF's annual authorization process.[25] Instead of describing the limitations or lack of penetration testing and the identified vulnerabilities, the applicable section in the SARs for both years stated, "No significant findings." This language incorrectly suggests that testing had been completed, when in fact it had not. Further, this same language in the 2023 SAR was not consistent with the actual results of NOAA's penetration tests conducted that year, which as previously stated found significant vulnerabilities.

The issues described above left gaps in penetration testing of the NCCF and provided an incomplete picture of risk to officials making the annual authority to operate decisions for the NCCF. Additionally, by only addressing instances of the issues discovered during penetration testing, NCCF developers re-introduced several serious security issues, which we used to attack the system, as further described below.

B. *Critical security weaknesses allowed OIG to take complete control of the NCCF system during penetration testing*

The Federal Information Security Modernization Act[26] mandates that agencies secure their information systems against potential threats by implementing effective security controls such as managing accounts, securing passwords and configurations, and addressing security weaknesses.

Our testing started from inside the NCCF's external security boundary (as a general user) and with knowledge of the system's design.[27] We found that critical security weaknesses allowed us to gain full administrative control of the system using only basic cyberattacks. Our exploitation of these security weaknesses identified 11 "critical" and 2 "high" severity issues.[28] See appendix A for a description of our testing scope and methodology.

Although the system had security controls, we bypassed the NCCF's security measures due to misconfigurations and inappropriate management of user accounts, associated passwords, and related security access keys.[29] Our attacks gained full system control and demonstrated that any internal user of the system could do the same with limited

[25] The SAR and annual authorization process were completed in August 2022.

[26] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (Dec. 18, 2014).

[27] This is a standard practice to simulate the knowledge and access an advanced persistent attacker could gain over time.

[28] We used the Common Vulnerability Scoring System, which provides a standardized method to rate the severity of security vulnerabilities in systems or software. The severity ratings indicate the level of risk a vulnerability poses to the organization's operations or security if exploited.

[29] A "security access key" refers to a specialized form of a digital credential, like a password, that is known only to its owner and is used to access systems and data.

technical knowledge and skills. Using these weaknesses, a basic user could manipulate data, modify system operations, and completely disable the system.

We also found that a basic user could obtain access to various NOAA and international partner systems. Because this is a cloud system, once we obtained the proper security access keys, we could access and control the system remotely from anywhere in the world.

Recommendations

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 POA&Ms in the security system of record.
    c. Penetration tests are conducted prior to the creation of the SAR that supports the annual authorization process.
    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).

IV. The NCCF Is Built on a Cloud Platform That Cannot Support its Security Requirements, Putting Critical Data at Risk

The NCCF processes and stores data that is critical to severe weather monitoring and prediction. Even though the NCCF is critical to NOAA's mission, it is currently operating on a cloud platform that cannot support its high security needs. Further, the NCCF is only hosted in one region of the country, which could affect its availability if a disaster or disruption occurs in that region. In contrast, the cloud service provider recommends considering a multi-region architecture to better ensure system availability.

A. The NCCF's current moderate-impact cloud platform cannot meet its high-impact system security requirements

Federal Information Processing Standards require all government IT systems to undergo a security categorization process based on three security objectives: availability, integrity, and confidentiality. The overall impact rating of the system (low, moderate, or high) is determined by the highest rating for any of the individual security objectives. The Federal Risk and Authorization Management Program (FedRAMP®) policy designates standardized security control requirements for cloud-based high-impact systems like the NCCF.[30]

The NCCF's security objectives for integrity and availability are rated high, and the objective for confidentiality is rated moderate. As such, the NCCF is categorized as a high-impact system.

Despite its high-impact rating, NESDIS built the NCCF on a moderate-impact rated cloud platform that lacked over 100 security controls required for a high-impact cloud platform. According to NESDIS personnel, the moderate-impact cloud platform chosen for the NCCF provided more flexibility for connecting outside users, including international partners, and was more cost effective than a high-impact cloud platform. NESDIS attempted to add security controls to meet its high-impact integrity and availability security objectives while remaining on the moderate-impact cloud platform.

The NCCF's moderate platform lacked **over 100 security controls** required for a high-impact cloud platform.

However, NESDIS' approach had fundamental flaws. The approach was based on an incorrect assumption that the moderate-impact cloud platform could satisfy the NCCF's high-impact requirements with added security controls. Several of the security controls that NCCF personnel wanted to add could only be performed by the cloud service provider. Examples include hard drive sanitization, long-term alternate power supplies, and testing contingency plans at alternate processing sites. Yet the cloud service provider does not offer these controls on its moderate-impact cloud platform that is currently used for the NCCF.

As a result, the NCCF continues to operate below the federal standard of protection for high-impact systems, putting critical data at risk.

B. *The NCCF's current cloud platform may not support its users' need for high system availability*

The NCCF needs to continuously provide up-to-date weather data to its users. The NCCF business impact analysis states that the NCCF has a high availability requirement, with a maximum tolerable downtime of only a few hours. The NCCF cloud service provider recommends that systems with short tolerable downtimes, such as the NCCF, consider using a multi-region cloud architecture.[31]

Notwithstanding this recommendation by the provider itself, the NCCF does not use a multi-region architecture and instead resides in a single region. OCS personnel noted

[30] FedRAMP® was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. In December 2022, the FedRAMP Authorization Act (Act) was signed as part of the National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263 (Dec. 23, 2022). The Act codifies the FedRAMP® program as the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information. See https://www.fedramp.gov/.

[31] Multi-region cloud architecture uses cloud resources (e.g., software and data) across multiple geographic regions to improve disaster recovery and mitigate the risk of an entire region going down.

that while the NCCF's cloud platform resides in a single region, the NCCF operates concurrently in two separate cloud facilities within that region. NOAA's analysis of alternatives for migrating to a cloud architecture did not include a multi-region scenario. OCS personnel did recognize that if a service disruption were to affect the entire region, the NCCF could be impacted.

Our research found that a service disruption impacting the NCCF did occur in 2023 that was close to the maximum tolerable downtime of the system. Additionally, prior to the NCCF, the region that currently hosts the NCCF had several service disruptions that lasted longer than the maximum tolerable downtime. Our analysis found that these disruptions have occurred roughly every 2 years.

Based on available documentation, we determined that OCS personnel did not thoroughly analyze the system's high-availability needs against real-world outage data to determine if their single-region architecture was appropriate. OCS personnel told us this single-region design provides better availability than NESDIS' legacy on-premises ground system architecture.

Despite this perceived improvement in availability, the NCCF is vulnerable to regional outages. If any part of the NCCF were to become inoperable longer than the maximum tolerable downtime, it would directly affect NOAA's ability to provide environmental data needed to protect lives and property from severe storms.

Recommendations

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

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.

Summary of Agency Response and OIG Comments

On August 2, 2024, we received NOAA's response to our draft report. NOAA concurred with all our recommendations and described actions it has taken, or will take, to address them. We are pleased that NOAA concurs with our recommendations and look forward to reviewing its formal action plan. NOAA's complete response is included in this report as appendix C.

Appendix A: Objective, Scope, and Methodology

Our audit objective was to assess NESDIS' progress implementing the NCCF. To satisfy our objective, we examined aspects of the management and execution of the NCCF effort as well as the extent to which existing security controls adequately protect the system from cyber threats.

To understand the current status of the program, we reviewed historical documentation for the NCCF, including reports, analysis, reviews, and program management documents. We compared information obtained against several commercial and government agencies' best practices and guidance to help focus our discussions with NESDIS officials.

To assess project management practices, we identified criteria from NESDIS policies and procedures. We collected and analyzed NCCF status reviews, financial data, and project planning documents and compared them to actual progress. We interviewed NCCF project management experts to understand the system's development, schedule, costs, performance, and the agile project management framework. We also held meetings with senior leaders to discuss the problems we found and to hear their views on why the problems occurred.

To understand why NOAA did not report the NCCF's financial, project, and performance data to the Federal IT Dashboard, we reviewed OMB's rules for reporting and interviewed NESDIS leadership and the Deputy Chief Information Officer for the Department regarding the relevance to the NCCF of the 2013 agreement to remove NESDIS' satellite ground systems from federal IT reporting requirements. We also reviewed the documented rationale for this agreement.

To determine the extent to which existing security controls adequately protect the system from cyber threats, we conducted three phases of fieldwork, described below. All IT assets inside the NCCF's authorization boundary were in scope for our penetration testing (e.g., cloud services, virtual servers).

Phase 1: Preparation. We reviewed the NCCF's security documentation, including past security assessments, penetration tests, vulnerability scans, and control assessments. We also conducted interviews and a system walkthrough with NCCF personnel, which provided insights into the system's architecture and operations. Based on these reviews, we pursued additional inspection of the NCCF's moderate-impact cloud platform and single-region architectural approaches (see Phase 3: Additional Fieldwork).

Phase 2: Penetration Testing. We conducted our penetration testing from November 7, 2023, to December 22, 2023. Our testing methodology assumed the external perimeter was breached and focused testing on what actions an adversary may or may not be able to achieve once inside the network. We probed the NCCF for weaknesses, then exploited them in attack chains to see whether and to what extent they could be used to negatively impact the NCCF mission. We performed additional fieldwork in areas where our attacks indicated security controls were deficient.

Phase 3: Additional Fieldwork. We conducted further investigations through interviews with NCCF staff and leadership, reviewed internal security assessments, POA&Ms and service tickets, and policies related to their penetration testing processes. From our initial documentation review, we assessed the NCCF's compliance with FedRAMP® requirements and analyzed its cloud architecture, focusing on its single-region approach and the implications of using multi-availability zones versus multi-region architecture. We also compared publicly available service outage data to the NCCF's current goals and availability requirements.

Throughout these phases, we aimed to gain a comprehensive understanding of the NCCF's security posture, identify areas of improvement, and assess the effectiveness of current security controls and procedures. Our testing may not have, however, identified every security vulnerability or weakness in the NCCF system.

Additionally, we assessed internal controls that are significant within the context of our objective through document reviews and interviews with key personnel to determine adherence to procedures and plans. Specifically, we reviewed monthly OCS program status reviews, quarterly reporting to the Program Management Council, POA&Ms, SARs, flow of requirements from NESDIS down to lower levels of the NCCF effort, adherence to cost and schedule baselines, and design and implementation of information security controls. Our findings and recommendations are inclusive of our internal control assessment.

Although we could not independently verify the reliability of all the information we collected, we compared it with other available supporting documents to determine data consistency and reasonableness. We also gathered computer-generated information like logs, standard output, and system alerts as part of our penetration testing and independently determined it was reliable. Based on these efforts, we believe the information we obtained is sufficiently reliable for this report.

We conducted our audit from August 2023 to July 2024 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401–424), and Department Organization Order 10-13, dated October 21, 2020. We performed our fieldwork remotely from the OIG office headquartered in Washington, DC.

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 our audit objective.

Appendix B: Potential Monetary Benefits

The table below presents the estimated costs of the NCCF for FYs 2025 and 2026. Implementing recommendations 1–4 will enable NOAA to control the effort more effectively, thereby putting these funds to better use.

Finding and Recommendation	Funds To Be Put To Better Use
Finding 1, recommendations 1–4	$98,000,000

Source: OIG analysis of NCCF documentation

Appendix C: Agency Response

NOAA's response to our draft report follows on p. 19.

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

FROM: Benjamin P. Friedman
Deputy Under Secretary for Operations
National Oceanic and Atmospheric Administration

Ben F
2024.08.02
10:49:39 -04'00'

SUBJECT: *A Lack of Program Management Controls and Attention to IT Security Threaten the Success of NOAA's Effort to Implement a Cloud-Based Common Ground System* – 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 Success of NOAA's Effort to Implement a Cloud-Based Common Ground System. 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 Lawrence N. Burney, Jr., Acting Director, Audit and Information Management Office on (202) 643-6010.

Attachment

NOAA AUDIT RESPONSES AND ACTION PLAN

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

Audit Report Number: Project No. OIG-2023-458/ July 2024

Audited Entity: National Environmental Satellite, Data, and Information Service (NESDIS)

OIG Recommendations #1 - 4: We recommend the NOAA Administrator direct the NOAA Deputy Under Secretary of Operations 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 as described in the DOC Acquisition Agile Program and Project Management Guidebook, including a formal lifecycle cost estimate; cost, schedule, and technical performance baselines; and performance measurement against those baselines.

3. Delivers official requirements to OCS for development of the NCCF.

4. Directs OCS to comply with all aspects of NESDIS requirements management policy, including establishment of a requirements management board to oversee requirements and creation of a requirements management plan for the NCCF.

Action Planned or Taken: We concur. To meet this end, NESDIS intends to take the following actions:

1. We concur. NESDIS will develop a management control approach for NCCF that is in accordance with Department of Commerce guidelines aligned with DAO 208-16.

2. We concur. The NESDIS established an Independent Review Board (IRB) to assess the NCCF development and started its independent review of the NCCF development at the end of July 2024. The NESDIS-level IRB will finalize its independent review of the NCCF against the DOC Acquisition Agile Program and Project Management Guidebook by late August 2024. OCS will use the independent review findings to inform the maturation of the formal management controls for the NCCF and the implementation strategy to align cost, schedule, and technical performance baselines of the NCCF investment.

3. We concur. NESDIS will define and deliver requirements for the development of the NCCF. The top-level requirements contained within the [in-baseline process] NESDIS Ground Enterprise (NGE) objectives document are based on clear architectural and operational baselines that define the NCCF. This NGE objectives document provides clear traceability of NCCF-relevant requirements within the objectives document to NCCF functional requirements. Those NCCF (NGE) requirements provide well-defined scope, thresholds, and objectives for OCS development processes.

4. We concur. NESDIS will comply with all aspects of NESDIS requirements management policy. The NESDIS enterprise requirements will be managed through an existing configuration control board that controls requirements baselines. NESDIS will establish and manage a lower level requirements configuration control board for NCCF and document the process in a requirements management plan.

Target Implementation Date: The entire process should be concluded by February 2025**.**

NOAA AUDIT RESPONSES AND ACTION PLAN

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

Audit Report Number: Project No. OIG-2023-458/ July 2024

Audited Entity: National Environmental Satellite, Data, and Information Service (NESDIS)

OIG Recommendation #5: We recommend the NOAA Administrator direct the NOAA Deputy Under Secretary of Operations to ensure NCCF financial, project, and performance data is reported to OMB via the Federal IT Dashboard, in accordance with federal budget guidance.

Action Planned or Taken:

5. We concur. NESDIS will evaluate federal criteria governing IT investment reporting to ensure the NCCF complies with relevant statutes, regulations, and guidance. This analysis will ensure differential categorization of IT investment for mission delivery vs. standard IT investments, in accordance with OMB guidance. NESDIS will continue monitoring and developing cloud computing reporting guidance and ensure submissions evolve to accurately capture all relevant aspects of the IT portfolio.

Target Implementation Date: March 2025.

NOAA AUDIT RESPONSES AND ACTION PLAN

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

Audit Report Number: Project No. OIG-2023-458/ July 2024

Audited Entity: National Environmental Satellite, Data, and Information Service (NESDIS)

OIG Recommendations #6 - 8: We recommend the NOAA Administrator direct the NOAA Deputy Under Secretary of Operations ensure NESDIS:

> **6.** Updates the NESDIS penetration testing process to ensure:
>
> > **6a.** Penetration testers have adequate access to examine all system components.
> >
> > **6b.** Penetration test findings are documented in POA&Ms in the security system of record.
> >
> > **6c.** Penetration tests are conducted prior to the creation of the SAR that supports the annual authorization process.
> >
> > **6d.** 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).

Action Planned or Taken: We concur. To address these recommendations, NESDIS will take the following actions:

> **6a.** We concur. As part of the formulation for Rules of Engagement (RoE) for penetration testing, the penetration testers are only excluded from out of bounds areas that may have a real-world mission impact via black listed IP address ranges. Their access to equipment depends on a variety of factors including if it is an on-site penetration test or off-site remote test, or whether it's a black box, gray box, or white box test.
>
> NESDIS will ensure that future penetration testers have access pertinent to the type of test being conducted; request timely status reports; and that any concerns are reported so they can be addressed before the end of the test.
>
> All relevant NESDIS penetration testing documentation will be updated to reflect any changes, and all personnel will be informed of the changes.

6b. We concur. NESDIS will ensure that any findings, including open or closed, minor or critical, will be reported to the Authorizing Officials during the systems' official Security Control Assessment (SCA) Brief. Plan of Action and Milestones (POA&Ms) will be created for any remaining open issues and reported in Cyber Security Assessment and Management (CSAM) system within 1 week (7 days) of the finding(s). The NESDIS Penetration Testing Standard Operating Procedure (SOP) will be updated to reflect the above changes and ensure relevant personnel are briefed.

6c. We concur. NESDIS will ensure penetration tests are scheduled prior to the SCA by aligning schedules and informing stakeholders that the Security Assessment Report (SAR) takes into account the previous Penetration Test and is not dependent on a future Penetration Test.

6d. We concur. NESDIS is given a penetration test report that covers all aspects of the test. NESDIS will ensure that processes and procedures are updated to cover any limitations to the test that were found, and if any impediments were encountered by the PenTest team while trying to exploit the system.

SAR reports have the penetration test results in them, however they are usually from the previous penetration test. Moving forward we will ensure that scheduling and activities are aligned and they are documented correctly.

7. We concur. OCS as the system owner will ensure consistent steps in the POA&M process to demonstrate root cause analysis and reporting closure of POA&Ms through the established organizational processes.

8. We concur. NESDIS conducted meetings and developed plans with system stakeholders to discuss findings, and to mitigate them as well as establish official POA&Ms listed in CSAM. All but one POA&M have been remediated successfully, checked for compliance and closed. The remaining open POA&M is currently in work and is dependent on partner schedules to complete. Most findings identified by the OIG were closed within a week. The others were closed in a timely manner with sufficient compliance artifacts.

NESDIS will ensure that the root cause is addressed by conducting an After-Action Review after the penetration test with system stakeholders, and that any changes are incorporated into the penetration test policies and procedures. This will ensure that whatever caused the finding(s) is solved and that system personnel are properly educated and trained to recognize these types of issues before they are elevated into real security concerns.

Target Implementation Date: The entire process will be concluded in September 2025 with the conclusion of the next Authorization to Operate (ATO) annual review cycle using the improved processes.

NOAA AUDIT RESPONSES AND ACTION PLAN

Audit Report Title: A Lack of Program Management Controls and Attention to IT Security Threaten the Success of NOAA’s Effort to Implement a Cloud-Based Common Ground System

Audit Report Number: Project No. OIG-2023-458/ July 2024

Audited Entity: National Environmental Satellite, Data, and Information Service (NESDIS)

OIG Recommendations #9 - 11: We recommend the NOAA Administrator direct the NOAA Deputy Under Secretary of Operations ensure NESDIS:

> **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.

Action Planned or Taken: We concur. To address these recommendations, NESDIS will take the following actions:

> **9.** Since the initial assessment of the NESDIS cloud platform by the OIG, NESDIS has found through continual assessments and analysis of the AWS documentation and consultations with AWS senior assessors, that the NCCF provides equivalent protection to that of the NIST High Security Baseline. Through the assessment and Authorization process NESDIS will ensure the NCCF continues to provide equivalent protections to a high impact cloud platform.
>
> By the target implementation date, the NCCF will be assessed at the 800-53 r5 controls which will demonstrate it meets the high impact cloud baseline.
>
> **10.** NESDIS will ensure all high impact controls are implemented in accordance with the requirements identified in the NIST 800-53 as amended and any related AWS Customer Responsibility Matrix documents.
>
> By the target implementation date, the NCCF will be assessed at the 800-53 r5 controls which will demonstrate it meets the high impact cloud baseline.
>
> **11.** NESDIS will review and update its analysis of alternatives to include moving to a multi-region architecture and document the cost-based decision(s) on NESDIS’ ability to meet availability requirements.

Target Implementation Date: The entire process should be concluded by September 2025 with the conclusion of the next ATO annual review cycle.

REPORT

FRAUD

& WASTE

ABUSE

HOTLINE

Department of Commerce

Office of Inspector General Hotline

www.oig.doc.gov | 800-424-5197