U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

National Oceanic and Atmospheric Administration

FY2009 FISMA Assessment of the Environmental Satellite Processing Center (NOAA5045)

Final Report No. OAE-19730

January 2010

Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

January 6, 2010

MEMORANDUM FOR: Dr. Jane Lubchenco
Under Secretary of Commerce for Oceans and
Atmosphere and NOAA Administrator

FROM: Allen Crawley
Assistant Inspector General
for Systems Acquisition and IT Security

SUBJECT: National Environmental Satellite, Data, and
Information Service (NESDIS)
FY 2009 FISMA Assessment of Environmental Satellite Processing Center (NOAA5045)
Final Report No. OAE-19730

Attached please find a copy of our report on the results of our evaluation of the Environmental Satellite Processing Center (ESPC). We evaluated certification and accreditation activities for ESPC as part of our responsibilities under the Federal Information Security Management Act (FISMA).

We found that NESDIS did not follow the required planning processes for certification and accreditation, and proper security planning has not taken place. We also found that the majority of required security controls are not in place and effective plans have not been developed to implement them. This is a particular concern because NESDIS has categorized ESPC as a high-impact system, which means a security breach could have severe or catastrophic adverse effects on organizational operations, organizational assets, or individuals.

Notwithstanding these significant security issues, ESPC is an essential NOAA system that supports critical mission requirements, and therefore must continue to operate. However, immediate management attention is needed to ensure that appropriate security controls are implemented to effectively protect this system.

NOAA's December 18, 2009, response to our draft report recommended several changes that disputed our findings and was receptive to just two of our five recommendations. The response itself was not consistent with NOAA's deputy chief administrative officer's statement, made in a transmittal memo, that NOAA agreed with our five recommendations after meeting with the Department OCIO, NOAA, and OIG to attempt to resolve disagreement over the findings and recommendations.

NOAA does concur that ESPC's security posture must improve. However, NOAA maintains that NESDIS followed the required process for C&A and that risk was properly identified and disclosed to the authorizing official. For this reason, NOAA was not responsive to our recommendations related to security planning, control assessment, and what circumstances were necessary before an accreditation decision could be properly made.

NOAA agrees with our recommendations to address system deficiencies through its revised plan of action and milestones process, and to revise the system's accreditation status to an interim authorization to operate. However, as we explain in our comments, NOAA's reasons for revising the system's accreditation status are not consistent with what we found during our evaluation.

In our report, we summarize and comment on NOAA's response and have included it in its entirety as appendix B. We ask that you consider our comments and craft an action plan accordingly for the recommendations to which NOAA did not agree.

Please submit an action plan to us within 60 calendar days from the date of this memorandum—this should be in the form of a plan of action and milestones, as required by FISMA.

We appreciate the cooperation and courtesies extended to us by your staff during our evaluation. If you would like to discuss any of the issues raised in this report, please call me at (202) 482-1855.

Attachment

cc: Mary M. Glackin, Deputy Under Secretary of Commerce for Oceans and Atmosphere
Suzanne Hilding, Chief Information Officer, U.S. Department of Commerce
Mary E. Kicza, assistant administrator for Satellite and Information Services, National Environmental Satellite, Data, and Information Service
Joe Klimavicz, chief information officer, National Oceanic and Atmospheric Administration
Zachary Goldstein, chief information officer, National Environmental Satellite, Data, and Information Service

Kathy Kelly, acting director, Office of Satellite Data Processing and Distribution, National Environmental Satellite, Data, and Information Service

Nancy DeFrancesco, IT security officer and chief, IT Security and Operations Division, National Environmental Satellite, Data, and Information Service

Mack Cato, director, Audit, Internal Control, and Information Management Office, National Oceanic and Atmospheric Administration.

Report In Brief

U.S. Department of Commerce, Office of Inspector General

December 2009

Why We Did This Review

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to identify and provide security protection of information collected or maintained by them or on their behalf. Inspectors general are required to annually evaluate agencies' information security programs and practices. Such evaluations must include testing of a representative subset of systems and an assessment, based on that testing, of the entity's compliance with FISMA and applicable requirements.

This review covers our evaluation of NOAA's ESPC, which is one of a sample of systems we assessed in FY 2009.

Background

ESPC is NOAA's primary processing system for the nation's environmental satellite data. ESPC ingests, processes, distributes, and archives data from two environmental and meteorological satellite systems.

C&A is a process by which security controls for IT systems are assessed to determine their overall effectiveness. Understanding the remaining vulnerabilities identified during the assessment is essential in determining the risk to the organizations's operations and assets, to individuals, to other organizations, and to the national resulting from the use of the system. Continuous monitoring is a critical post-accreditation aspect of this process.

National Oceanic and Atmospheric Administration (NOAA)

FY 2009 FISMA Assessment of the Environmental Satellite Processing Center (ESPC) (OAE-19730)

What We Found

Our objectives for this review were to determine whether (1) implemented controls adequately protected the system and its information, (2) continuous monitoring is keeping the authorizing official sufficiently informed about the operational status and effectiveness of security controls, and (3) the certification and accreditation (C&A) process produced sufficient information about remaining system vulnerabilities to enable the authorizing official to make a credible, risk-based accreditation decision.

We found that the National Environmental Satellite, Data, and Information Service has not followed the required process for C&A of ESPC. The lack of proper security planning undermined the effectiveness of the system's security certification, hindering the authorizing official in making a credible risk-based accreditation decision. The system's plan of action and milestones for remediating vulnerabilities is ineffective.

What We Recommend

We recommend that NOAA complete security planning activities, conduct appropriate security control assessments, and address system deficiencies. Until these activities have been completed, NOAA should revise the system's accreditation status to an interim authorization to operate.

In its response to our draft report, NOAA disputed our findings and concurred with only two of our recommendations. NOAA does agree that ESPC's security posture must improve. We have asked NOAA to reconsider its response based on our comments in this report and craft its action plan, due in 60 days, accordingly.

Contents

Introduction

The Environmental Satellite Processing Center (ESPC) is the National Oceanic and Atmospheric Administration's (NOAA's) primary processing system for the nation's environmental satellite data. Created by combining two systems, ESPC ingests, processes, distributes, and archives data received from satellites associated with the Polar-orbiting Operational Environmental Satellite, Geostationary Operational Environmental Satellite, and the European Meteorological Operational Satellite programs. It distributes environmental data to the National Weather Service, the U.S. Navy's and the U.S. Air Force's primary forecast centers, international forecast centers, academia, and the private sector.

The system provides critical weather information necessary for analyzing environmental conditions and predicting weather events and climatological changes. Therefore, ESPC is categorized as a high-impact system, which means that a security breach could have severe or catastrophic adverse effects on organizational operations, organizational assets, or individuals.

We evaluated certification and accreditation (C&A) activities for ESPC as part of our FY 2009 responsibilities for conducting independent evaluations under the Federal Information Security Management Act (FISMA). For our complete objectives, scope, and methodology, see appendix A.

Background

In FY2008, we reviewed the Satellite Environmental Processing System (SATEPS), one of two systems that were incorporated into ESPC. In our report, *FY 2008 FISMA Assessment of Satellite Environmental Processing System (OSE-19167),* we noted that SATEPS, which was also a high-impact system, operated for at least 2 years with significant deviations from mandatory security requirements before it was decommissioned. The National Environmental Satellite, Data, and Information Service's (NESDIS') own assessments showed that 85 percent of the required security controls were not in place. While we were concerned about NESDIS management's attention to IT security, we agreed with NESDIS' decision to extend SATEPS' authorization to operate; it would have been too costly to reaccredit the system only to decommission it a short time later.

In response to our report, NESDIS asserted that the extension allowed funds to be used instead to certify and accredit ESPC, and that SATEPS was not a typical example of NESDIS' IT security practices. However, NESDIS' security certification of ESPC demonstrated that significant security issues remain. NESDIS' own certification team assessed ESPC controls between June 2007 and January 2008 and found that

- 87 percent (118 of 135) of the security controls that should be implemented by the system owner were not in place;

- among those not implemented were 6 of 7 identification and authentication controls, 14 of 15 account management (including user access rights) controls, 10 of 10 audit and accountability controls, and 8 of 8 configuration management controls;
- vulnerability scans of 548 components identified 55 unique high- and 128 unique moderate-severity vulnerabilities (Note: raw counts were not specified.);
- scanning of 25 web applications found a total of 4,275 vulnerabilities including 72 "critical," 1285 high-, and 1698 medium-severity vulnerabilities (assessors were also not confident that application scanning was comprehensive because installed software was not tracked in the system's inventory);
- network diagrams for the system were exposed on the Internet, and testers were able to successfully bypass authentication controls; and
- the inventory of system components in the accreditation boundary was incomplete.

The summary provided in the security assessment report, initially issued in February 2008 by NESDIS' own certification team, states,

> The defects identified during the Certification and Accreditation process are indicative that the ESPC is not ready to operate as an integral partner in the NOAA mission support system and needs significant management adjustment to meet the minimums for any Federal system, and even more significant adjustment to meet the needs for supporting and sustaining the intended mission. The state of the system security indicates that the integration process totally neglected the statutory and regulatory requirements for Federal operating systems under a misguided impression that prior neglect justifies continued neglect of the security posture.

Despite ESPC's numerous security problems, it was granted an interim authorization to operate on February 15, 2008. NESDIS subsequently

- reassessed the system component inventory and found 281 components that had not been identified, thus increasing the component count by about 45 percent;
- scanned 884 of the 907 system components and found 83 unique high-severity vulnerabilities (each component had at least one high-severity vulnerability) and 228 unique moderate-severity vulnerabilities (increases from 55 and 128 respectively);
- developed an intrusion detection system implementation plan and implemented a limited, initial capability; and

- created plan of action and milestones (POA&M) items to track the remediation of control weaknesses.

Following completion of these activities, NESDIS granted ESPC an authorization to operate on April 15, 2008. However, even though these activities were important, our review found that only minor improvements to system security had been made.

Summary of NOAA Response and OIG Comments

NOAA Response

In response to our draft report, NOAA's deputy chief administrative officer indicated that NOAA was in agreement with the five recommendations in the draft report. However, our review of NOAA's response indicates disagreement with our findings and is non-responsive to three of our five recommendations. NOAA agrees with our recommendations to address system deficiencies through its revised plan of action and milestones process and to revise the system's accreditation status to an interim authorization to operate.

NOAA acknowledged that security must improve for ESPC and that such improvements are in progress. However, NOAA indicated that we did not consider an April 2009 report of a study commissioned by NESDIS, "which provides a strategy for mitigating ESPC's high-risk plans of action and milestones (POA&Ms)." NOAA asserted that NESDIS follows National Institute of Standards and Technology (NIST) guidance for the C&A process to identify the system's residual risk, but the guidance has no requirement indicating "which security controls must be fully implemented in order for the system to receive a full authorization to operate."

NOAA also recommended we remove the quoted section of its security assessment report from the "Background" section on page 1, because it was "the opinion of the assessor and [does] not reflect the official decision of the authorizing official."

We summarize NOAA's response in the appropriate sections of the report and include the response in its entirety as appendix B.

OIG Comments

NOAA disagreed with our findings related to the certification and accreditation of ESPC. NESDIS' management did not dispute our underlying findings when we presented them at an exit conference in September, but did disagree with our conclusions. We reaffirm our findings, and explain our rationale accordingly:

1. The April 2009 study was outside the scope of our evaluation—the study had no bearing on the certification and accreditation of the system, the review of continuous monitoring activities conducted in March 2009, the implementation of security controls at the time of our evaluation, or the POA&M process. NOAA, in its response, did not explain how the study would have changed our findings. However, during our field work we did question NESDIS management about it and were told that the study presented a number of options for management to take, but an option has not been selected.

2. NOAA's contention that NESDIS follows the NIST Special Publication (SP) 800-37 C&A process is not consistent with what we found during the course of our evaluation. As described in the report and in our comments to NOAA's response, NESDIS did not conduct key aspects of security planning that are necessary for an effective control assessment, providing assurance that vulnerabilities have been appropriately identified.
3. With regard to NOAA's suggestion that we omit the quoted section of its security assessment report from the "Background" section of this report, the security assessment report presents the independent findings of the certification team as to the state of the system's security controls. Therefore, it is appropriate to include in our report; this is the nature and value of independent assessment. The quotation provides a sense of what the certification team found, particularly with respect to the ESPC C&A process and compliance with requirements for federal systems; it also suggests a pattern of behavior consistent with previous findings from our review of SATEPS.

Correction

In the "Background" section of the Introduction, the draft report incorrectly stated the number of system components NESDIS identified after reassessing its system inventory was "more than 300." The actual number was 281 and the final report has been corrected accordingly. The percentage increase remains 45 percent, as stated in the draft and final reports.

Edits

We have also edited the background section to better quantify the results of NESDIS' security certification, including the number of controls not implemented and the extent and results of vulnerability scanning.

Change to Recommendation

In our draft report, we recommended that NOAA report the system as not certified and accredited in the Department's system inventory. Our intent was to raise senior management's attention and bring additional oversight to this critical, high-impact system, which has virtually no meaningful IT security controls in place. However, after meeting with NOAA officials and the Department OCIO, we now recommend that NESDIS change the accreditation status to an interim authorization to operate. NOAA's CIO plans to grant a waiver from Department policy that will allow the system to operate under an interim authorization, beyond the 90-day limit currently allowed by Department policy. The Office of Management and Budget (OMB) does not consider systems operating under an interim authorization to be accredited; this (and our December 2009 meeting with NOAA and the OCIO) will bring increased attention to ESPC's information security.

Findings and Recommendations

NESDIS did not follow the required C&A planning processes, and still has not completed proper security planning. The lack of defined security requirements undermined the certification team's ability to assess controls accurately and completely. With no system-specific security requirements, the certification team was forced to judge controls against generic control statements. In addition, although federal information systems have required certain security controls for several years, most of the requisite controls for this high-impact system are not yet in place, nor has NESDIS developed an effective implementation strategy for them.

I. Proper Security Planning Did Not Take Place, Undermining the Certification and Accreditation Process

Since 2005, Department policy has required operating units to follow the C&A process detailed in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. NIST SP 800-37 outlines a four-phased process[1] to ensure "agency officials have the most complete, accurate, and trustworthy information possible on the security status of information systems." The first phase, initiation, includes security planning activities intended to provide a basis for assessing security controls in the security certification phase.

As we found in our evaluation of SATEPS, NESDIS has not finished the necessary planning to implement minimum security controls. ESPC's security certification process began before NESDIS completed adequate security planning. Specifically, the system accreditation boundary was poorly defined, the system security plan did not describe the implementation of controls (i.e., the tailored security requirements) required for a high-impact system, and the implementation status of the controls (whether a control is planned or in place) was unknown.

In its draft corrective action plan,[2] used in support of the accreditation decision, NESDIS' first corrective action to be addressed was to identify security requirements for the system. The plan describes problems arising from a lack of security requirements and states,

> The un-documented state of the current ESPC environment coupled with a lack of detailed end-state definition of the ESPC environment precludes the development of detailed, engineering level technical solutions, detailed component configurations and settings. As such,

[1] The four phases of the C&A process are initiation, security certification, security accreditation, and continuous monitoring.

[2] In a briefing to the authorizing official that recommended the system be granted an approval to operate, this draft plan was cited as evidence that ESPC has demonstrated that plans are in place to correct significant issues. NESDIS still has not finalized its corrective action plan.

additional documentation and studies should be conducted to be able to recommend a solution.

NESDIS' lack of security planning undermined the effectiveness of the security certification. In accordance with NIST SP 800-37, control assessments are conducted to determine whether controls are implemented effectively and to provide the authorizing official with enough information to make a credible, risk-based decision to approve system operation. Assessments should determine whether controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system's security requirements. However, NESDIS primarily used the results of control assessments as a security planning tool—to help identify if and how security controls were implemented—when this information should be known in advance so that assessment procedures can be crafted to determine the controls' effectiveness.

The majority of controls could not be properly assessed because system-specific security requirements were not documented. For example, there were no defined auditable events for the system, no assessable account management procedures, and no defined secure configuration settings for IT products; the assessors concluded that these controls "failed."

The only appropriate corrective action in these instances was for the system owner to identify specific security requirements for the system, a task that, had the required process been followed, would have been completed before the security certification began. Therefore, most of ESPC's control assessments stated only that no system-specific implementation requirements had been defined—a fact that NESDIS was aware of before the security certification phase.

NOAA Response

NOAA disagreed that a lack of defined security requirements undermined the certification team's ability to assess controls adequately and completely; instead, controls were assessed "against the NIST SP 800-53 baseline and fully disclosed the risks associated with absent or ineffective controls."

The bureau disputed our finding that NESDIS has not completed the necessary security planning and asserted that it had completed the initiation phase tasks from NIST SP 800-37; the tasks included "documenting the security categorization and the [system security plan…which] indicates which controls are implemented and which are not." NOAA also argued that NIST guidance does not require all controls be implemented before completing the initiation phase, only that the status of controls be reflected in the system security plan, which in ESPC's case, was done.

NOAA said that we misinterpreted its corrective action plan (quoted in the report) when we said that the plan describes problems arising from a lack of security requirements. NOAA contended the "plan is describing ESPC's architectural deficiencies, not shortfalls in requirements definition," which "are not relevant to the C&A planning process."

NOAA disagreed with our finding that NESDIS primarily used the results of control assessments as a security planning tool. It said the "primary purpose was to make a risk-based assessment of whether to accredit the system for continued operation." It noted that the authorizing official first granted an interim authorization to operate and then, after "improvements were made that allowed fuller understanding of the security posture" and increased system security, the assessment results were used to justify the authorization to operate and prioritize short- and long-term actions needed to improve the system's security.

OIG Comments

While NOAA's certification team assessed ESPC security controls against the NIST SP 800-53 baseline, the certification team did not have the benefit of an accurate system inventory, tailored control requirements, and system- or component-specific descriptions of implemented controls. These details, which result from security planning commensurate with a high impact-level system like ESPC, would have allowed the team to craft meaningful assessment procedures for the various IT products with some assurance that all components were being assessed beyond basic vulnerability scanning.

NESDIS may have "completed" initiation phase tasks in some manner, but contrary to NIST SP 800-37, control assessments were conducted before NESDIS fully defined the accreditation boundary and meaningfully documented security controls in the system security plan. Simply indicating "which security controls are implemented and which are not" is not adequate security planning, particularly for a high-impact system; even that much was not done until after the certification assessments were completed. In addition, as we state in the report, the assessment results often amounted to recommendations that NESDIS identify specific security requirements for the system. Had the required process been followed, the specific security requirements would have been identified before security certification began. As such, the control assessments were ineffective at identifying operational and technical vulnerabilities that may exist within ESPC system components.

We make no assertions as to what extent controls must be implemented in order to complete the initiation phase, only that controls must be documented to the extent they are planned or implemented. We found that NESDIS did not follow the Department's process for C&A. As a result, the authorizing official lacked sufficient information about the system's remaining vulnerabilities, regardless of the fact that the authorizing official may have believed there was an acceptable, albeit significant, level of risk.

Section 4.0, "Corrective Actions-Technical," of NESDIS' *Draft Corrective Action Plan* describes deficiencies in five security control families, deems these deficiencies "most critical," and includes the section we quoted in our first finding. The certification agent, in a briefing to the authorizing official, referred to this plan to address the security deficiencies. However, regardless of what the purpose of the document is, the quote itself is a clear illustration of problems arising from a lack of

security requirements: "un-documented state…lack of detailed end-state definition of the ESPC environment precludes the development of detailed…component configurations and settings."

With respect to our finding that NESDIS used control assessments as a security planning tool, such assessments began on the system before the status of security controls was known—the certification team verified this, and it was also evident in multiple documents in the C&A package. In some instances, we identified the certification team's assessment results used as descriptions of controls in later versions of the system security plan. As such, it is clear that NESDIS used the certification assessments as a starting point to identify if and how security controls were implemented, which is a planning activity rather than a determination of effectiveness.

II. The Majority of the Required Security Controls for This High-impact System Are Not in Place

Our review of the current system security plan and continuous monitoring activities shows security posture has improved little since ESPC was authorized to operate. The plan indicates that 70 percent (94 of 134) of required security controls that should be implemented by the system owner—including those related to user identification and authentication, user access rights, system and application event auditing, and configuration management—are still not in place. However, 16 of the 40 security controls labeled "in place" have open POA&M items describing significant deficiencies. Factoring these items into the status count increases the amount of controls not in place to 82 percent.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, describes minimum security control requirements that have been Department policy since 2006 and Federal Information Processing Standards (FIPS 200) since 2007. NIST SP 800-53 outlines minimum assurance requirements for a high-impact system like ESPC:

> The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control (including functional interfaces among control components).

The current security plan only describes security control deficiencies and does not include implementation descriptions that address the intended solution or plans to address the deficiency. The POA&M items ESPC has created to address these control deficiencies typically refer to generic NIST SP 800-53 control requirements rather than system-specific security requirements.

NESDIS is currently reassessing security control ownership to determine which controls are the responsibilities of the ESPC system owner and which are provided by other systems. Determining control ownership is a key security planning activity that should have been completed in the initiation phase.

As we found in our review of SATEPS (now incorporated into ESPC), most of ESPC's required security controls are not in place and have not been for some time. NIST SP 800-37 states, "Information systems*, especially mission-critical or high-impact systems* [emphasis added] as described in FIPS 199, should not be operating with significant security vulnerabilities requiring extended remediation time." Yet NESDIS' current plans indicate that some critical controls will not be effectively implemented until the system is recertified in 2011. Because ESPC is mission critical, it must continue to operate. Since it is also high impact, it is imperative that appropriate security controls be implemented promptly.

NOAA Response

NOAA suggested we omit the paragraph in this finding that addresses NESDIS' efforts to reassess security control ownership. This reassessment, said NOAA, is not related to initiation phase security planning activities; instead it is "driven by…re-architecting of ESPC and an evaluation of the appropriateness of establishing …common controls supporting multiple systems, of which ESPC is one." Such analyses are ongoing and long-term in nature, and "one would not expect [them] to be completed within a certification initiation phase."

OIG Comment

We found that controls deemed the responsibility of ESPC's system owner (as evidenced by the security plan, security assessment report, and POA&M) during the C&A process were, in fact, not considered system-specific controls by NOAA officials with direct responsibility for ESPC security. Therefore, in accordance with NIST SP 800-37, the issue of common controls should have been resolved before the initiation phase was completed.

III. ESPC's POA&M Process Is Ineffective and Does Not Support Continuous Monitoring

ESPC staff explained that when the two systems were merged to create ESPC, POA&M items from both systems were combined to form the ESPC system POA&M. We found that many of the POA&M items were duplicative or inaccurate. In addition, ESPC staff said they no longer add deficiencies identified through vulnerability scanning to the POA&M. Instead, these vulnerabilities are assigned to system administrative staff for remediation. However, the same vulnerabilities are often identified in subsequent scans, indicating that corrective actions are frequently not taken.

Our review of ESPC's POA&M items found that descriptions of weaknesses are often vague and actions required to close an item not clearly specified. Also, many items describing similar weaknesses had different planned completion dates, which hindered prioritizing corrective actions. Of 136 POA&M items that were closed (indicating corrective actions had been completed) between January 1 and July 29, 2009, we found that about 40 percent were (1) considered invalid by ESPC staff, (2) closed due to a lack of information about the vulnerability, or (3) found to be duplicative and deferred to POA&M items scheduled to be completed later. Thus, closing these items did not actually correct deficiencies in the system.

Several of the closed POA&M items we reviewed were related to deficiencies in controls associated with system event auditing. After reviewing evidence submitted as proof that the deficiencies had been corrected, we questioned the justification for closing the items. ESPC staff conceded that the deficiencies had not actually been corrected and told us the POA&M items had been erroneously closed. We also learned that additional items may have been closed in error, raising uncertainty as to the effectiveness of some controls purportedly addressed in the remaining 60 percent of the closed POA&M items.

NESDIS briefs the authorizing official monthly about the number of POA&M items completed, and the briefings do state, "POA&M statistics may not reflect accurate risk to NESDIS or mitigation of status to NOAA, DOC, or OMB." NESDIS recently developed policies and procedures intended to improve the quality of system POA&Ms. However, the current POA&M, which has not incorporated the new procedures, is ineffective in tracking vulnerabilities and prioritizing corrective actions.

NOAA Response

NOAA did not comment on this finding in its response to our draft report.

Conclusion

While ESPC's controls clearly do not adequately protect the system and its information, the true extent of vulnerabilities is unknown because of inadequate security planning. An undefined accreditation boundary, undefined security requirements, unspecified control implementations, and uncertainty over control ownership are conditions that must be resolved before a focused and effective assessment of controls, producing credible information about system vulnerabilities, can occur. This is particularly important for a high-impact system.

NESDIS should have reported the system as unaccredited until it had completed both security planning and, thereafter, an effective assessment of controls. The Department's C&A process requires that the requisite planning occur before controls can be meaningfully assessed and before an accreditation decision can be made. NESDIS did not do the security planning—in particular, fully documenting the system's security requirements— necessary to support security certification and the subsequent accreditation decisions, both on an interim basis and later, without restrictions.

The Department and NOAA's senior leadership should be concerned about management's lack of attention to IT security. The lack of security planning has persisted for too long, and the decision to accredit this system seems to have been made despite little meaningful change to the system's security posture.

NOAA Response

NOAA disagreed with our conclusion, saying "the report draws incorrect connections between security planning and vulnerability disclosure." NOAA disagreed that management lacks attention to security and offered the system owner and authorizing official's attention to "changes required to obtain the accreditation," the implementation of an alternate processing facility, and the re-architecting of the system (in progress) as proof of "sustained, long-term effort needed to make fundamental improvements in the security posture." NOAA asserted that the "the certification assessment fully disclosed the extent of vulnerabilities, the accreditation decision was properly informed, and the system was appropriately reported as accredited."

OIG Comments

As we state in the conclusion, there was an "undefined accreditation boundary, undefined security requirements, unspecified control implementations, and uncertainty over control ownership" at the time the certification team assessed controls. While the certification team did identify some significant weaknesses, the true extent of vulnerabilities cannot be known without resolving these ambiguities.

NOAA's contention that we "[draw] incorrect connections between security planning and vulnerability disclosure" contradicts the logical application of the C&A process described in NIST SP 800-37. This guidance makes a clear distinction between

security planning and an independent assessment of controls and supports our position that security planning is a necessary precursor to effective control assessment. We found that NESDIS did not perform adequate security planning, and this logically resulted in an ineffective assessment of controls. In fact, as we describe in our first finding, the lack of security planning negatively affected the assessment of controls, notably auditable events, account management, and secure configuration settings of IT products.

It is important to note the contradictions in NOAA's response. NOAA did not dispute these aspects of our second finding: there are virtually no meaningful controls in place and the current system security plan does not accurately describe the status of controls, address security requirements, or meet the assurance requirements for a high-impact system. Likewise, NOAA agrees that the mechanism for tracking and correcting security deficiencies (its POA&M) is ineffective. Therefore, NOAA did not dispute that two of the three key information inputs to the accreditation decision—the system security plan and the POA&M—were deficient.[3] At the same time, it is NOAA's position that the process to certify and accredit the system was appropriately followed, the true extent of the system's vulnerabilities was disclosed, and the accreditation decision was properly informed.

[3] According to NIST SP 800-37, the authorizing official uses a "security accreditation package" consisting of the system security plan, the security assessment report and the POA&M to determine the risk to agency operations, agency assets, or individuals.

Recommendations

To ensure that ESPC has adequate IT security protection, NESDIS should

1. complete security planning activities for ESPC in accordance with Department policy and FISMA requirements;
2. conduct security control assessments against the properly defined, system-specific security control requirements;
3. use its newly developed POA&M policies and procedures to develop POA&M items to address system deficiencies;
4. make the accreditation decision after determining system risk based on remaining vulnerabilities; and
5. revise the system's accreditation status to an interim authorization to operate until these activities have been completed.

NOAA Response

In a paragraph before its responses to our specific recommendations, NOAA indicated it did not agree with those "related to the process followed and decision to accredit ESPC because they are misleading regarding the manner in which NESDIS implemented the federal policy for the ESPC C&A." NOAA asserted that it "performed the proper tasks in the correct sequence to certify and accredit ESPC," and that the authorizing official has the sole discretion for the accreditation decision.

1. For recommendation 1, NOAA "agree[d]" that NESDIS needs to complete all initiation phase requirements, but it believed it had done so for ESPC. It further stated that NESDIS will complete security planning "again" for the recertification and accreditation of ESPC scheduled in April 2011.
2. For recommendation 2, NOAA "agree[d]" that ESPC control assessments "followed the approved controls baseline as documented in the [system security plan]." It further stated that NESDIS issued a policy on August 31, 2009, that formally documents its security control assessment methodology.
3. For recommendation 3, NOAA concurred and stated that "implementation of this recommendation is already underway…proper documentation and management of POA&Ms is a critical element of continuously monitoring the effectiveness of security controls." NOAA requested the specific POA&Ms that we found had been closed inappropriately.
4. For recommendation 4, NOAA indicated it "concur[red]" but stated that the "accreditation decision for ESPC was made after a determination of system risk, and this risk was disclosed to the authorizing official." It further stated that NESDIS issued a policy, on August 31, 2009, for its C&A process.

5. For recommendation 5, NOAA concurred because our findings related to the system's POA&M have raised "additional uncertainty," which "creates an unacceptable risk." The authorizing official will change the accreditation status to an interim authorization to operate through April 2011, which is when the original 3-year authorization expires. NOAA's CIO will issue a waiver from Department policy that limits interim authorizations to a period of 90 days. By doing so, NOAA agreed the system will be reported as not accredited (OMB does not consider systems with interim authorizations to operate to be accredited).

OIG Comments

In her transmittal of NOAA's response, the deputy chief administrative officer indicated that NOAA was "in agreement with the five recommendation[s] in the report." However, NOAA's actual response indicates disagreement with our recommendations that stems from disagreement with our underlying findings. We have addressed NOAA's disputes with our findings above. To NOAA's assertion that it performed the required tasks in the correct sequence, our report documents that it had not completed many of the tasks before testing began. Thus, the proper sequence was not followed. With respect to NOAA's responses to our recommendations, we add:

1. Recommendation 1: NOAA was not responsive to our recommendation that it undertake, presently, the security planning necessary to properly implement and then test security controls. Waiting until April of 2011, or a few months leading up to then, is not sufficient attention to activities that are necessary for the proper implementation of controls for a high-impact system. NOAA misconstrued the intent of the recommendation. We reaffirm our recommendation and ask senior management to provide an action plan that gives security planning the attention needed.
2. Recommendation 2: NOAA was not responsive to this recommendation, which was intended to correct the inadequacies of its security certification after first completing security planning per recommendation 1. NOAA's assertion that its "assessment followed the approved controls baseline as documented by the [system security plan]," even if true, would still not be adequate for a high-impact system like ESPC. NESDIS did not complete its security plan before control assessments began, and left unfinished the security planning activities we described in our report. As we documented, this failure compromised the control assessment—and thus the identification of vulnerabilities—necessary for a high-impact system. Further, NESDIS' August 2009 policies for control assessments have no relevance on our findings from activities that occurred in previous years. We reaffirm our recommendation and request NOAA reconsider and craft its action plan accordingly.

3. Recommendation 3: NOAA agreed. The POA&M items we identified that had been inappropriately closed were 28197, 28191, 28198, 18199, 28204, 28139, 28140, 28141, and 28212. These POA&M items are not inclusive of all NESDIS POA&Ms; they are just from those we sampled. Also, we did not review evidence for all closed POA&Ms in our sample, only ones that had obvious conflicts either with information provided to justify the closing, or from significant conflicts in the current system information that casts doubt as to the validity of the closing. As a result, there may be more erroneously closed POA&Ms than those listed here.
4. Recommendation 4: NOAA was not responsive to this recommendation, which was intended to be the next sequential step after our recommendations 1, 2, and 3. Instead, NOAA asserted that NESDIS followed the required process. It asserted that NOAA's August 2009 policy for C&A was followed even though ESPC's C&A concluded in April 2008. We reaffirm this recommendation and respectfully request NOAA reconsider and modify its action plan accordingly.
5. Recommendation 5: NOAA concurred with this recommendation, which was modified after a meeting between NOAA, the Department CIO, and OIG. However, NOAA's rationale, as described in its response, indicates that OIG's findings brought to light additional uncertainties associated with the POA&M process. We found that NOAA officials were well aware of problems with ESPC's POA&M and note in the report monthly briefings to the authorizing officials had a disclaimer: "POA&M statistics may not reflect accurate risk to NESDIS or mitigation of status to NOAA, DOC, or OMB." During the course of our evaluation NOAA personnel also acknowledged that there are problems with ESPC's POA&M and at our exit conference, NOAA officials unanimously agreed with our POA&M finding. All of these indicate that uncertainties concerning the progress of ESPC's POA&Ms were well known to management when we issued our draft report.

Appendix A: Objectives, Scope, and Methodology

We evaluated certification and accreditation activities for ESPC as part of our FY 2009 reporting responsibilities under FISMA.

Our objectives were to determine whether (1) implemented controls adequately protect the system and its information, (2) continuous monitoring is keeping the authorizing official sufficiently informed about the operational status and effectiveness of security controls, and (3) the certification and accreditation process produced sufficient information about remaining system vulnerabilities to enable the authorizing official to make a credible, risk-based accreditation decision.

Security certification and accreditation packages contain three elements, which form the basis of an authorizing official's decision to accredit a system:

- The **system security plan** describes the system, the requirements for security controls, and the details of how the requirements are being met. The security plan provides a basis for assessing security controls and also includes other documents such as the system risk assessment and contingency plan, per Department policy.
- The **security assessment report** presents the results of the security assessment and recommendations for correcting control deficiencies or mitigating identified vulnerabilities. This report is prepared by the certification agent.
- The **POA&M** is based on the results of the security assessment. It documents actions taken or planned to address remaining vulnerabilities in the system.

The Department's *IT Security Program Policy and Minimum Implementation Standards* requires that C&A packages contain a certification documentation package of supporting evidence of the adequacy of the security assessment. Two important components of this documentation are

- the **certification test plan**, which documents the scope and procedures for testing (assessing) the system's ability to meet control requirements; and
- the **certification test results**, which is the raw data collected during the assessment.

To evaluate the certification and accreditation, we reviewed all components of the certification and accreditation package, examined the system's POA&M items that were generated from certification and accreditation, and interviewed NESDIS staff to clarify any apparent omissions or discrepancies in the documentation and gain further insight on the extent of the security assessment. We evaluated the security plan and assessment results for applicable security controls and will give substantial weight to the evidence that supports the rigor of the security assessment when reporting our findings to OMB.

To evaluate the system security controls and continuous monitoring, we reviewed continuous monitoring assessment results and the updated system security plan that ESPC staff asserted incorporated continuous monitoring efforts. We requested additional information and evidence about controls during the course of our review to gain further insight on the status of controls. We also reviewed the system POA&M items that were closed during the calendar year. Because so few technical, operational, and management controls were implemented we opted not to perform our own on-site assessments of ESPC security controls, which we would typically do and which we would weigh significantly when determining the effectiveness of system security controls.

We used the following review criteria:

- Federal Information Security Management Act of 2002 (FISMA)
- U.S. Department of Commerce *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005 and *IT Security Program Policy,* March 9, 2009
- NIST Federal Information Processing Standards (FIPS)
    - Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
    - Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publications:
    - 800-18, *Guide for Developing Security Plans for Information Technology Systems*
    - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
    - 800-53, *Recommended Security Controls for Federal Information Systems*
    - 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
    - 800-70, *Security Configuration Checklists Program for IT Products*
    - 800-115, *Technical Guide to Information Security Testing and Assessment*

We conducted our evaluation in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections* (revised January 2005), issued by the President's Council on Integrity and Efficiency.

Appendix B: NOAA Response

UNITED STATES DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
CHIEF ADMINISTRATIVE OFFICER

December 18, 2009

MEMORANDUM FOR: Allen Crawley
Assistant Inspector General for Systems
Acquisition and IT Security

FROM: Sandra R. Manning
Deputy Chief Administrative Officer

SUBJECT: *FY 2009 FISMA Assessment of the Environmental Satellite Processing Center (NOAA5045)*
Draft Report No. OAE-19730/October 2009

The National Oceanic and Atmospheric Administration appreciates the opportunity to respond to your draft report on the Federal Information Security Management Act review of the Environmental Satellite Processing Center's (ESPC) certification and accreditation and security control continuous monitoring. We agree that the security posture of ESPC requires improvement, and we are committed to the long-term actions needed to improve its security.

During the December 10, 2009 meeting with officials from the Department of Commerce, National Oceanic and Atmospheric Administration, and Office of Inspector General, efforts were made to resolve issues for this review. As a result, we are in agreement with the five recommendation in the draft report. Our revised response is attached, which was prepared in accordance with Department Administrative Order 213-2, *Inspector General Inspections and Evaluations*.

Attachment

Department of Commerce
National Oceanic and Atmospheric Administration
Comments on the Draft OIG Report Entitled
"FY 2009 FISMA Assessment of the Environmental Satellite Processing Center (NOAA5045)"
(OAE-19730/October 2009)

General Comments

The National Oceanic and Atmospheric Administration (NOAA) appreciates the opportunity to review the draft Office of Inspector General (OIG) report on the National Environmental Satellite, Data, and Information Service's (NESDIS) Environmental Satellite Processing Center (ESPC). We agree that the security posture of ESPC requires improvement, and efforts are underway to implement these improvements. However, the draft report does not consider the "NOAA - ESPC IT Assessment Study," which provides a strategy for mitigating ESPC's high-risk plans of action and milestones (POA&Ms). IBM was commissioned by NESDIS to conduct this study and issued a report on April 17, 2009.

NESDIS also follows the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 certification and accreditation (C&A) process – thoroughly identifying and disclosing the residual risk of the system's security posture to the authorizing official so that he/she can consider this risk in the accreditation decision. Current federal guidelines do not provide specific guidance as to which security controls must be fully implemented in order for the system to receive a full authorization to operate. The requirement is that the risk be identified and disclosed to the authorizing official for consideration in making the accreditation decision. NESDIS followed this approach to accredit the ESPC system.

Recommended Changes for Factual/Technical Information

Page 2:
NOAA recommends the removal of opinion statements from the ESPC C&A security assessment report in the OIG report. Such statements represent the opinion of the assessor and do not reflect the official decision of the authorizing official. Therefore, this entire section of text should be removed from the report.

Page 3, first paragraph:
The draft report's conclusion that "the lack of defined security requirements undermined the certification team's ability to assess controls accurately and completely" is incorrect. NOAA performed certification assessment against the NIST SP 800-53 baseline and fully disclosed the risks associated with absent or ineffective controls.

Pages 3-4, section I:
The first sentence of the second paragraph on page 3 which states, "As we found in our evaluation of SATEPS, NESDIS has not finished the necessary planning to implement minimum security controls." is not accurate. The criteria cited for this section are the NIST SP 800-37 security planning activities for the C&A Initiation Phase. In accordance with NIST SP 800-37, NESDIS followed the

Initiation Phase activities of the C&A process. Specifically, NESDIS completed the Preparation task (Task 1), consisting of documenting the system's security categorization, assessed the system for risk, and documented the security controls baseline. NESDIS also completed the Notification and Resource Identification task (Task 2) activities by providing necessary notifications and identifying adequate resources for the C&A. For the System Security Plan (SSP) Analysis, Update, and Acceptance task (Task 3), NESDIS completed all required activities, including documenting the security categorization and the SSP. The SSP indicates which controls are implemented and which are not. NIST SP 800-37 does not require that all controls be implemented as part of this task, but that their status be reflected in the SSP, which was completed.

Page 3, last paragraph:
The OIG statement, "The plan describes problems arising from a lack of security requirements…" misinterprets the section cited from ESPC's first corrective action plan. This plan is describing ESPC's architectural deficiencies, not shortfalls in requirements definition. These architectural deficiencies arose over time and will take a long time to resolve. They are not relevant to the C&A planning process.

Page 4, first full paragraph, last sentence:
We disagree with the report's conclusion that "NESDIS primarily used the results of control assessments as a security planning tool – to help identify if and how security controls were implemented." The primary purpose was to make a risk-based assessment of whether to accredit the system for continued operation. The authorizing official's first decision was not to accredit the system but allow continued operation under an interim authority to operate. When improvements were made that allowed fuller understanding of the security posture as well as strengthening system security, the control assessment results were used to both accredit the system and prioritize the short and long-term actions needed for further security improvement.

Page 5, second full paragraph:
NOAA recommends this paragraph, addressing security control ownership, be deleted. The reassessment of security control ownership is not related to the security planning activities of the initiation phase. NESDIS' reassessment is driven by a number of factors, including the re-architecting of ESPC and an evaluation of the appropriateness of establishing some security controls as common controls supporting multiple NOAA systems, of which ESPC is one. These are ongoing, long-term analyses which one would not expect to be completed within a certification initiation phase.

Page 6, Conclusion:
We disagree with the report's conclusion. First, we disagree with the report's assessment that "the true extent of vulnerabilities is unknown because of failures in security planning." Second, the report draws incorrect connections between security planning and vulnerability disclosure. Third, we disagree that management lacks attention to security. On the contrary, the changes required to obtain the accreditation, implement an alternative processing facility, and to re-architect the system demonstrate the system owner's and authorizing official's commitment to the sustained, long-term effort needed to make fundamental improvements in the security posture. Finally, the certification assessment fully disclosed the extent of vulnerabilities, the accrediting decision was properly informed and the system was appropriately reported as accredited.

Editorial Comments

Page 9, fourth bullet under NIST Special Publications:
Change the publication number from "800-53" to "800-53A." NIST SP 800-53, which has a different title, is already listed as the third bullet.
Memorandum to NOAA, page 2, second to sixth names on distribution list:
All position titles for the officials listed should have initial capital letters (e.g., Assistant Administrator and Chief Information Officer).
Memorandum to NOAA, page 2, seventh name on distribution list:
Replace "Lisa Lim, National Oceanic and Atmospheric Administration audit liaison" with "Mack Cato, Director, Audit, Internal Control, and Information Management Office, NOAA."

NOAA Response to OIG Recommendations

We fully support the general principles for implementing the C&A process in accordance with NIST SP 800-37; however, we do not concur with the OIG recommendations related to the process followed and decision to accredit ESPC because they are misleading regarding the manner in which NESDIS implemented the federal policy for the ESPC C&A. The draft report asserts NOAA did not comply with Department of Commerce (DOC) and Federal Information Security Management Act (FISMA) requirements and improperly accredited ESPC. We respond that NOAA performed the proper tasks in the correct sequence to certify and accredit ESPC. More importantly, as a matter of policy, accreditation is a risk acceptance decision at the sole discretion of an authorizing official.

Recommendation 1: "To ensure that ESPC has adequate IT security protection, NESDIS should complete security planning activities for ESPC in accordance with Department policy and FISMA requirements."

NOAA Response: We agree that NESDIS needs to complete all NIST SP 800-37 requirements for the C&A Initiation Phase of the ESPC C&A. NESDIS believes all NIST SP 800-37 requirements for the C&A Initiation Phase of the ESPC C&A were done, but NESDIS will complete security planning activities again for the C&A scheduled in April 2011.

Recommendation 2: "To ensure that ESPC has adequate IT security protection, NESDIS should conduct security control assessments against the properly defined, system-specific security control requirements."

NOAA Response: We agree that the security control assessments of ESPC conducted for purposes of annual assessment and certification assessment followed the approved controls baseline as documented in the SSP. *NESDIS Policy and Procedures for Conducting Security Controls Assessments*, dated August 31, 2009, was issued to formally document the security assessment methodology of NIST SP 800-53A implemented within NESDIS.

Recommendation 3: "To ensure that ESPC has adequate IT security protection, NESDIS should use its newly developed POA&M policies and procedures to develop POA&M items to address system deficiencies."

NOAA Response: We concur. Implementation of this recommendation is already underway. We agree that proper documentation and management of POA&Ms is a critical element of continuously monitoring the effectiveness of security controls. Furthermore, NOAA requires the specific

POA&Ms numbers that the OIG found to be closed inappropriately so that we can reassess the status and open new POA&Ms as necessary.

Recommendation 4: "To ensure that ESPC has adequate IT security protection, NESDIS should make the accreditation decision after determining system risk based on remaining vulnerabilities."
NOAA Response: We concur**.** The accreditation decision for ESPC was made after a determination of system risk, and this risk was disclosed to the authorizing official. *NESDIS Certification and Accreditation Process Policy and Procedures*, issued on August 31, 2009, describes how NESDIS implements the C&A process in accordance with NIST SP 800-37.

Recommendation 5: "To ensure that ESPC has adequate IT security protection, NESDIS should report the system in the Department's system inventory as not certified and accredited until these activities have been completed."

NOAA Response: We concur. The OIG's findings related to the ESPC POA&M have brought to light additional uncertainty associated with POA&M progress reporting, due to the overall complexity of the POA&M. The magnitude of the current POA&M work remaining creates an unacceptable risk to the program, and the authorizing official is changing ESPC's accreditation status to an Interim Authority to Operate (IATO) through April 2011. Because of the importance of focusing all appropriate resources on restructuring and then working the POA&M, the NOAA Chief Information Officer is approving a waiver to DOC policy limiting IATOs for high impact systems to 90 days. Therefore, we agree the system will be reported as not accredited.