



**U.S. DEPARTMENT OF COMMERCE**  
**Office of Inspector General**

---



***NATIONAL OCEANIC AND  
ATMOSPHERIC ADMINISTRATION***

***Progress Being Made in  
Certification and Accreditation Process,  
but Authorizing Officials Still Lack  
Adequate Decision-making Information***

*Final Report No. OSE-18019/September 2006*

*Office of Systems Evaluation*





**UNITED STATES DEPARTMENT OF COMMERCE**  
**The Inspector General**  
Washington, D.C. 20230

SEP 19 2006

**MEMORANDUM FOR:** Conrad C. Lautenbacher, Jr.,  
Undersecretary of Commerce for Oceans and Atmosphere and  
NOAA Administrator

John J. Kelly, Jr.  
Deputy Undersecretary of Commerce for Oceans and Atmosphere

**FROM:**

Johnnie E. Frazier

**SUBJECT:**

*Progress Being Made in Certification and Accreditation Process,  
but Authorizing Officials Still Lack Adequate Decision-making  
Information*  
Final Inspection Report No. OSE-18019

As follow-up to our draft inspection report, attached is our final report presenting findings from our FY 2005 Federal Information Security Management Act (FISMA) review of three NOAA C&A packages. Our review found that while NOAA made progress, further enhancement is needed to improve its C&A process.

This report presents the findings from our FY 2005 review of the following packages: the Search and Rescue Satellite-aided Tracking system (SARSAT), the Polar Orbiting Operational Environmental Satellite Ground System (POES), and the Office of Response and Restoration Seattle Local Area Network (Seattle LAN). Each of these systems was certified by NOAA personnel and accredited by a senior NOAA official as part of NOAA's C&A improvement effort.

Our report focuses on two problem areas we identified in the three systems reviewed. The first is the lack of sufficiently complete system descriptions to ensure adequate identification and examination of system components in security control assessments. The second is inadequate security control assessments, which did not evaluate many of the system controls and were conducted without adequate test procedures. Consequently, NOAA's certification process did not provide sufficient information to authorizing officials on remaining vulnerabilities.

In its written response to our draft report, NOAA agreed with most of our recommendations, but took issue with two of them, and suggested one factual change. In the response, NOAA also noted that C&A activities for both POES and SARSAT were completed nearly 14 months ago and stated that subsequent to our December 5, 2005 exit briefing, the bureau made immediate changes in its C&A process. NOAA stated that it has implemented most of the changes recommended in our report.



Based on NOAA's response, we have made changes to the report that should result in NOAA's full agreement with both the recommendations and content. The summary section of the report describes these changes. With respect to the time lag in issuing this report, we reemphasize that some of the problems we identified in our FY 2005 and previous reviews were still evident in the additional five NOAA C&A packages we reviewed early in FY 2006. We briefed the NOAA CIO and appropriate line office officials on these problems at the beginning of FY 2006. Our hope is that documenting our concerns in this report will further facilitate correction of these issues, many of which have persisted for some time.

We appreciate the cooperation of NOAA staff during our evaluation, and are pleased with NOAA's response. The actions NOAA has identified in its written response should be recorded on a plan of action and milestones (POA&M) as required by FISMA and provided to me within 60 calendar days.

If you would like to discuss this report, please contact me at (202) 482-4661, or Judith Gordon, Assistant Inspector General for Systems Evaluation, at (202) 482-5643.

Attachment

cc: Greg Withee, Assistant Administrator for Satellite and Information Services  
John H. Dunnigan, Assistant Administrator for NOAA Oceans and Coasts  
Carl Staton, Chief Information Officer, National Oceanic and Atmospheric Administration

## CONTENTS

Summary .....	i
Introduction.....	1
Objectives, Scope, and Methodology .....	3
Findings and Recommendations .....	5
I. NOAA Has Enhanced System Security Plans and Risk Assessments, but Additional Improvements Are Needed .....	5
A. Security Plans Improved, but System Descriptions Need to Be More Accurate....	5
B. Risk Assessments Provided More Useful Information.....	6
Recommendations.....	8
II. Security Control Assessments Were Not Sufficient for Effective Certification...	10
A. Vulnerability Scanning Was Incomplete and Ineffective .....	10
B. Security Control Assessments Did Not Provide Evidence of Effective Management, Operational, and Technical Controls .....	13
Recommendations.....	15
APPENDIX: NOAA's Response.....	17

## SUMMARY

This report presents the findings from our FY 2005 Federal Information Security Management Act (FISMA) review that relate to important parts of NOAA's certification and accreditation (C&A) process: 1) system security plans/risk assessments, and 2) security control assessments.

System certification is the comprehensive assessment of security controls implemented in an information system. It determines the extent to which controls are implemented correctly, operating as intended, and meeting the security requirements for the system. Accreditation is management's formal authorization to allow a system to operate and includes an explicit acceptance of the risk posed by the identified remaining vulnerabilities.

For FY 2005, we reviewed the C&A documentation for three NOAA systems: the Search and Rescue Satellite-aided Tracking system (SARSAT), the Polar Orbiting Operational Environmental Satellite Ground System (POES), and the Office of Response and Restoration Seattle Local Area Network (Seattle LAN). Each of these systems was certified and accredited as part of NOAA's C&A improvement effort.

As we noted in our September 2005 *Semiannual Report to Congress*, NOAA had significantly improved risk assessments, security plans, and security control assessments. Our review found, however, that further enhancement is needed to improve its C&A process. Our FY 2005 independent FISMA evaluation reported that C&A packages for SARSAT and the Seattle LAN were compliant with FISMA, but POES was not. However, even for SARSAT and the Seattle LAN, several important aspects of the C&A process need to be improved. We have prepared this report to highlight problems with the SARSAT, POES, and the Seattle LAN C&As that we have seen in other NOAA packages in prior years and were still evident in our review of five NOAA systems earlier in FY 2006.

NOAA has categorized SARSAT and POES as high-impact systems because a security breach would potentially have severe or catastrophic adverse effects. The certification and accreditation of SARSAT and POES should therefore reflect the highest degree of rigor. The Seattle LAN, as a moderate impact system, would be held to a somewhat lesser standard but a significant degree of due diligence should be manifest in the C&A process.

### **NOAA Has Enhanced System Security Plans and Risk Assessments, but Additional Improvements Are Needed.**

Security plans form the basis for certification activities by outlining the security requirements for a system and the controls put in place to meet the requirements. NOAA security plans were improved from those we saw in our FY 2004 review with more accurate accreditation boundaries and better identification of software components and interconnections. But the plans failed to accurately depict network components—raising the possibility that certification efforts may not adequately examine such devices. Current

interconnection agreements were not in place for POES and SARSAT. Without formal interconnection agreements, there are insufficient mechanisms for enforcing security requirements on external systems with which NOAA systems are connected, posing increased risks to the agency and agency operations.

Risk assessments for all three systems provided useful information for NOAA system owners to determine what appropriate security controls should be, although we noted some flaws in the assessment methods. Often, the threats and vulnerabilities assessed were vague or broad generalizations and the analysis at times confused the definitions of the terms. The analysis of how controls may mitigate specific adverse events was also lacking. Under recent NIST standards and guidance for selecting security controls, risk assessments should focus on tailoring the security control baseline as well as analyzing any resource-intensive changes to the security features of the system. (See page 5.)

We recommend NOAA ensure security plans provide a complete and accurate account of system components and interconnection agreements are in place. And NOAA should ensure risk assessments are used to tailor security control baselines and provide analysis and justifications for resource-intensive changes to the security features of the information system. (See page 8.)

### **Security Control Assessments Were Not Sufficient for Effective Certification.**

NOAA's use of vulnerability scans to assess the adequacy of security controls was incomplete and ineffective. NOAA's designated scanning tool was unable to evaluate many network components for all three systems. POES scans were successfully completed on only 4 of 14 components residing on its development network, while the operational network was not scanned. SARSAT scans were also limited—key components such as firewalls, routers, and switches were not scanned prior to the accreditation. Additional scans of POES and SARSAT conducted in response to our concerns were also incomplete.

NOAA did not analyze or correct potentially serious vulnerabilities on the Seattle LAN. Although two additional scanning tools were used and identified a significant number of vulnerabilities, the vulnerabilities were not analyzed or corrected prior to the accreditation decision, and they were not identified to the authorizing official.

Although POES and SARSAT are high impact systems that require penetration testing, such testing was not performed. Penetration testing can provide an indication of how vulnerable an organization's network is and the level of damage that can result.

Security control assessments did not provide evidence of effective management, operational, and technical controls. POES, SARSAT, and the Seattle LAN control assessments covered only a subset of the minimum security controls described in NIST guidance. Generally, the C&A packages did not include specific procedures for evaluating the controls or adequate documentation of the results. Moreover, the approach used to select network components for technical control assessments did not provide for

complete testing of all operating system variants running on servers, workstations, laptops, routers, and switches. (See page 9.)

We recommend NOAA ensure comprehensive vulnerability scanning, analyze and document scan results, and plan and implement penetration testing on high-impact systems. NOAA should comprehensively test all management, operational, and technical controls, perform technical control tests on each operating system variant, and clearly document remaining vulnerabilities for the authorizing official. (See page 14.)

### **Summary of NOAA's Response**

In response to our draft report, NOAA concurred with most of our recommendations, but took issue with two of them. In regards to our recommendation that component listings be comprehensive and consistent with results of network scanning, NOAA agreed that security plans should provide an accurate and comprehensive listing of components. However, the bureau argued that “perfect line-by-line consistency between a vulnerability scan and the component listing, while desirable, is seldom achievable,” and provided two reasons why components would not be scanned due to technical or operational circumstances. The bureau stated that to ensure vulnerability scanning is as comprehensive as possible, it would “analyze and explain identified discrepancies between component listings and vulnerability scans performed during certification testing.”

NOAA took exception with our recommendation pertaining to the sampling approach used to test systems, based on the bureau's interpretation of the recommendation to be more exhaustive than we had intended. The bureau suggested we change the wording of the recommendation by replacing the word “identically” with “uniquely.”

NOAA recommended one factual change to our report, pertaining to the vulnerabilities discovered by scans of the Seattle LAN. The bureau recommended we change one sentence to reflect the fact that the vulnerabilities were addressed on the system's Plan of Action and Milestones (POA&M) “that covered all risks accepted by the authorizing official.” It noted that the POA&M entries, “generally stated that vulnerabilities were discovered by scanners and needed correcting and/or mitigating.”

NOAA made the point that the C&A activities for the three systems we reviewed had begun 18 months prior and were completed 14 months ago. NOAA stated that it made immediate changes in its C&A process subsequent to our December 2005 briefing on the same subject matter. The bureau also stated that it has now fully adopted NIST guidance, implemented enhanced internal review processes, added C&A support staff, and increased risk analysis and reporting requirements. NOAA leadership has worked, “to raise awareness of the resources required to implement and maintain an effective and compliant C&A program.” As such, the bureau believes it has implemented most of our recommendations and will continue to take steps to, “ensure program effectiveness.”

## **OIG Comments**

In regards to our recommendation that component listings should be comprehensive and consistent with results of network scanning, we concede NOAA's point that perfect line-by-line consistency is a difficult task. However, the reasons NOAA provided really describe two scenarios where the scans would not identify components included in the system security plan. Our review also found the opposite: scans identified components that were not included in the security plan, thus drawing into question the completeness of the system description. This is important because it raises the possibility that other required testing (beyond vulnerability scanning) will not be performed on devices omitted from the security plan, but which are, in fact, a part of the system. That said, we are satisfied with NOAA's intention to analyze and explain discrepancies between scans and component listings, so long as the outcome achieves an accurate depiction of the system and leads to comprehensive certification testing.

With respect to our recommendation pertaining to the sampling approach used to test systems, we have changed the wording according to NOAA's suggestion. As a result, the bureau should fully concur with our recommendations.

In regards to the scan results for the Seattle LAN, we have changed the sentence on page 11 according to NOAA's suggestion. However, we have also added a sentence indicating that the POA&M entries, which were general statements that vulnerabilities were discovered by scans, were not sufficient to describe the nature of the risks found by the scans and that such is more appropriately described in the security assessment report.

Lastly, while we recognize that this report details findings from work NOAA did over a year ago, its publication was motivated by preliminary reviews of five additional C&A packages early in FY 2006, which identified similar problems. Our hope is that documenting our concerns in this report will further facilitate correction of these issues, many of which have persisted for some time. We are generally pleased with NOAA's response and feel that we have made changes to the draft which should rectify the issues NOAA raised. We look forward to the output from NOAA's improved C&A process including the enhanced security that should result.

NOAA's written response is included in its entirety as an appendix to this report.



## INTRODUCTION

Pursuant to the Federal Information Security Management Act (FISMA), we evaluated selected aspects of NOAA's information security program in FY 2005. This report presents our findings that relate to important parts of NOAA's certification and accreditation process: 1) system security plans/risk assessments, and 2) security control assessments.

### NOAA's C&A Improvement Effort

On February 24, 2005, the Department CIO issued a plan to eliminate Commerce's IT security material weakness by having improved C&A packages by the end of FY 2005 for all national-critical systems, along with a substantial number of mission-critical systems. All Commerce systems were to have acceptable quality C&A packages by the end of FY 2006. Accordingly, in FY 2005 NOAA began an effort to improve its certification and accreditation process.

For FY 2005, we reviewed the certification and accreditation of three NOAA systems: the Search and Rescue Satellite-aided Tracking system (SARSAT), the Polar Orbiting Operational Environmental Satellite Ground System (POES), and the Office of Response and Restoration Seattle Local Area Network (Seattle LAN). Each of these systems was certified and accredited as part of NOAA's improvement effort.

As we noted in our September 2005 Semiannual Report to Congress, NOAA had significantly improved risk assessments, security plans, and security control assessments. Our review found, however, that while NOAA made progress, further enhancement is needed to improve its C&A process. Our FY 2005 independent FISMA evaluation reported that C&A packages for SARSAT and the Seattle LAN were compliant with FISMA, but POES was not. However, even for SARSAT and the Seattle LAN, several important aspects of the C&A process need to be improved. We have prepared this report to highlight problems with the SARSAT, POES, and the Seattle LAN C&As that we have seen in other NOAA packages in prior years and were still evident in our review of five NOAA systems<sup>1</sup> earlier in FY 2006. We have briefed NOAA on our findings for these five systems, some of which are scheduled to be resubmitted for our FY 2006 FISMA evaluation.

### Security categorizations of NOAA systems

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, defines three levels of potential impact on organizations or individuals in the event of a security breach—high, moderate, and low. NOAA categorizes SARSAT and POES as high-impact systems because the loss of

---

<sup>1</sup> NOAA0200 Network Operations Center (NOC), NOAA0300 Message Operations Center (MOC), NOAA3070 Geophysical Fluid Dynamics Laboratory, NOAA6205 Physical Oceanographic Real-Time System (PORTS) and National Water Level Observation Network (NWLON), and NOAA6501 Office of Coast Survey (OCS) Nautical Charting System.

confidentiality, integrity, or availability is expected to have severe or catastrophic effects. The Seattle LAN is categorized as a moderate-impact system because a security breach would have a lesser but still serious adverse effect. A security breach of a low impact system would be expected to have a limited adverse effect.

The security categorization of a system sets the initial baseline of minimum security controls found in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, which is now required under the Department's IT security policy, updated in June 2005.<sup>2</sup> Security categorization is important not only for the resulting control requirements, it should also guide the rigor, intensity, and scope of all information security-related activities—including those that constitute the certification and accreditation process.

As high impact systems, the certification and accreditation of SARSAT and POES should reflect the highest level of effort in defining security requirements and implementing controls, assessing the effectiveness of those controls, and proactively identifying and managing security weaknesses. The Seattle LAN, as a moderate impact system, would be held to a somewhat lesser standard but a significant degree of due diligence should be manifest in the C&A documentation.

#### The goal of certification and accreditation

System certification and accreditation is a key element of agency information technology (IT) security programs. Certification is the comprehensive assessment of security controls implemented in an information system. It determines the extent to which controls are implemented correctly, operating as intended, and meeting the security requirements for the system. Through the formal assessment of controls, the system certifier identifies remaining vulnerabilities—vulnerabilities not eliminated by the implementation of security controls.

Accreditation is management's formal authorization to allow a system to operate and includes an explicit acceptance of the risk posed by the identified remaining vulnerabilities. Through accreditation, senior agency officials take responsibility for the security of the systems over which they have management, operational, and budget authority and for any adverse impacts should a breach in security occur.

---

<sup>2</sup> For FY 2005, systems had the option of meeting the minimum controls in 800-53 or NIST SP 800-26, *Security Self-Assessment Guide for Information Technology*. All three NOAA systems we reviewed described the 800-53 controls in their security plans or control assessments. POES and SARSAT also included controls from 800-26. Federal Information Processing Standard Publication 200, *Minimum Security Requirements for Federal Information Systems*, now makes the minimum security controls specified in NIST SP 800-53 mandatory (non-waiverable) for federal agency systems.

## OBJECTIVES, SCOPE, AND METHODOLOGY

The purpose of this report is to discuss key findings for NOAA from our FY 2005 independent FISMA evaluation and to provide recommendations based on these findings. As shown in Table 1, we reviewed selected C&A packages<sup>3</sup> from the National Environmental Satellite Data and Information Service (NESDIS) and National Ocean Service (NOS).

Table 1. OIG Review Coverage by NOAA Line Office

NESDIS	Search and Rescue Satellite-aided Tracking (SARSAT)—NOAA 5023
NESDIS	Polar Orbiting Operational Environmental Satellite Ground System (POES)—NOAA 5026
NOS	Office of Response and Restoration Seattle Local Area Network (Seattle LAN)—NOAA 6702

We reviewed three NOAA C&A packages for our FY 2005 evaluation.<sup>4</sup> During the course of our review, we discussed questions that arose with appropriate NOAA officials.

Our review criteria included:

- Federal Information Security Management Act of 2002 (FISMA)
- U.S. Department of Commerce, *IT Security Program Policy and Minimum Implementation Standards* (January 2003 or June 2005 versions, as applicable)
- U.S. Department of Commerce, System Security Plan Certification and Accreditation Package (SSPCAP) Requirements Inspection Checklist, version 2, June 30, 2003
- OMB Circular A-130, *Management of Federal Information Resources*
  - Appendix III, *Security of Federal Automated Information Resources*

---

<sup>3</sup> The Department's IT security policy defines a certification and accreditation package as a system security plan, risk assessment, contingency plan, incident response plan, configuration management plan, system interconnection agreements, security assessment report, certification work plan, certification test plan, certification test results, and a plan of action and milestones.

<sup>4</sup> Based on schedules provided by the Department's CIO Office, we expected 13 NOAA C&A packages to be available by our cutoff date, but received only 3. We did not include one NOAA package made available because OIG staff had previously provided feedback during its preparation. Hence, we believe subsequently evaluating it for FISMA compliance would be contrary to the requirement that our review be independent. The Seattle LAN package was the most acceptable of four additional packages provided after our cutoff date and was thus chosen to add to our review sample for FISMA reporting.

- National Institute of Standards and Technology's (NIST's) Federal Information Processing Standards (FIPS)
  - Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
  
- NIST Special Publications:
  - 800-18, *Guide for Developing Security Plans for Information Technology Systems*
  - 800-26, *Security Self- Assessment Guide for Information Technology*
  - 800-30, *Risk Management Guide for Information Technology Systems*
  - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
  - 800-42, *Guideline on Network Security Testing*
  - 800-53, *Recommended Security Controls for Federal Information Systems*
  - 800-63, *Electronic Authentication Guideline*
  
- Office of Management and Budget (OMB) Memoranda:
  - M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*

We conducted our evaluation in accordance with the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency in 2005 and under the authority of the Inspector General Act of 1978, as amended. We conducted our review from August 2005 to December 2005.

## FINDINGS AND RECOMMENDATIONS

### I. NOAA Has Enhanced System Security Plans and Risk Assessments, but Additional Improvements Are Needed

System security plans provided a better basis for certification activities than plans we reviewed in FY 2004. In particular, we saw improvements in the descriptions of accreditation boundaries, software components, and interconnections. But NOAA should improve identification of network components and obtain interconnection agreements, which are important for maintaining adequate security between systems. Risk assessments had also improved, providing a better identification of specific risks. Under the evolving NIST standards and guidance, the role of risk assessments has changed; we provide some comments on how they can be better utilized in the future.

#### A. Security Plans Improved, but System Descriptions Need to Be More Accurate

NOAA clearly delineated the major components of the accreditation boundary in its security plans, but some network components within the boundary were not always identified—raising the possibility that certification efforts may not adequately examine such devices. (See box for Departmental direction on system descriptions.)



Vulnerability scanning performed during certification of POES, SARSAT, and the Seattle LAN revealed network components not identified on the component listings in the systems' security plans. The security plan for the Seattle LAN listed 170 network components, but NOAA's primary network scanning tool reported 140 components scanned and a supplementary network scanning tool identified 202 network components. Scanning of the POES network identified 11 components not documented in its component listing. And five servers (i.e., key components) identified in SARSAT's scans were missing from the system topology diagram.

The component listing in the POES system security plan included identical names for different network components, making it impossible to discern which components were actually tested.

*POES and SARSAT lack interconnection agreements*

Our review of POES and SARSAT found that current interconnection agreements, as required by Appendix III to OMB Circular A-130, *Security of Federal Automated Information Resources* and Department policy, were not in place. The system security plan for SARSAT described five network interconnections, but SARSAT's C&A package included only a single, *unsigned* interconnection agreement with the Federal Aviation Administration.

Likewise, the POES system security plan indicated an interconnection agreement in place with the National Aeronautics and Space Administration, but it was not provided with the C&A package. The POES C&A package did include a signed MOU with a contractor, but the security plan indicated this particular interconnection agreement was "TBD" (to be determined).

If not appropriately safeguarded, interconnections with other systems may lead to breaches of security. Without formal interconnection agreements, there are insufficient mechanisms for enforcing security requirements between systems and as a result, increased risks to the agency and agency operations.

***B. Risk Assessments Provided More Useful Information***

Risk assessments of SARSAT and POES ultimately identified specific risks and control recommendations upon which system owners could take action. The lengthy assessments were prepared by a NOAA contractor and considered a broad range of threats and vulnerabilities that were factored into an extensive matrix ranking system.

While the assessments generally followed the NIST process, we found some faults at various steps in the process. Descriptions of many of the threats and vulnerabilities were vague or broad generalizations. In some cases, vulnerabilities were confused with threats (and vice versa) or consequences of vulnerability exploits. The sections describing controls did not consider how controls mitigated the likelihood of a particular adverse event, as NIST guidance requires.

However, the results summaries of both risk assessments identified system-specific vulnerabilities and included discussion of potential attacks and consequences. In most cases, recommendations for controls were made. Additionally, the results of technical vulnerability scans were included in the assessments. Although the scanning itself was very limited (see Finding II), the vulnerabilities identified in the scans were analyzed, prioritized, and system patches or other remediation measures were suggested.

Seattle LAN Risk Assessment

The Seattle LAN risk assessment listed one vulnerability/threat-source pair for each NIST SP 800-53 control (i.e., one adverse event per control). But according to NIST guidance, the analytical method is to consider a vulnerability/threat-source pair and the controls (i.e., multiple) in place or planned that may mitigate the risk. By only considering one potential adverse event per control, the analysis was incomplete—precluding consideration of *defense in depth*, a security principle that advocates the layering of controls to provide multiple defenses against various types of attacks. However, the assessment did summarize four risks and included a “safeguard implementation plan” that prioritized the risks, outlined remediation efforts, and detailed resources required and dates.

Risk assessments should focus on specific threats and vulnerabilities

The security categorization mandated by FIPS PUB 199 and corresponding minimum controls found in NIST SP 800-53 have changed the scope of risk assessments. The 800-53 security controls address the broader spectrum of threats and vulnerabilities that apply to all systems, including those pertaining to continuity of operations (which are also addressed in the system’s contingency plan).

Therefore, instead of considering all possible risks, NOAA risk assessments should focus on specific threats, vulnerabilities, and relevant security controls. These assessments should provide insight into the need for making changes to controls or control requirements. More specifically, risk assessments, including any related cost-benefit analysis, should be used as justification for tailoring the baseline of controls required by NIST SP 800-53 and for making resource-intensive changes to the security features of the information system.

Scoping guidance in NIST SP 800-53 describes risk-related considerations that may call for adjusting the baseline of minimum controls (in many cases by adding controls). Specific controls are listed as candidates for downgrading to a lower baseline. Doing so would require the action be consistent with the confidentiality, integrity, and availability impact levels of the system, and in many cases, be supported by a formal assessment of risk.

A security control assessment may reveal vulnerabilities that are easily corrected (e.g., by installing simple patches or updates) and others that require significant investment in time and resources to remedy. The former would need minimal analysis and should be quickly remedied. The more significant (particularly in terms of cost) vulnerabilities should be considered in the risk assessment, resulting in a statement of risk, recommendations for changing or adding controls, and cost-benefit analysis as appropriate. The system owner and authorizing official can then decide which needed changes deserve priority over others and guide resources accordingly.

### **Recommendations**

The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions for all C&A packages:

1. Ensure that security plans provide a complete and accurate account of system components.
  - a. Component listings should be comprehensive and consistent with results of network scanning performed during certification testing.
  - b. Network topology diagrams should include all key components and be consistent with network scan results.
  - c. Components should be uniquely identified so that certification activities can be accurately performed and tracked.
2. Ensure interconnection agreements or memoranda of understandings are obtained and included in future C&A packages.
3. Ensure risk assessments are used to tailor security control baselines and provide analysis and justifications for resource-intensive changes to the security features of the information system.

### **NOAA's Response**

In regards to our recommendation that component listings be comprehensive and consistent with results of network scanning, NOAA agreed that security plans should provide an accurate and comprehensive listing of components. However, the bureau argued that "perfect line-by-line consistency between a vulnerability scan and the component listing, while desirable, is seldom achievable," and provided two reasons why components would not be scanned due to technical or operational circumstances:

- If a device in the inventory is old or unique, it may be unknown to the vulnerability scanner software.
- A device in the inventory may be unavailable due to maintenance or removal from the system during the scan. An example of this is a laptop that is taken on travel.

The bureau stated that to ensure vulnerability scanning is as comprehensive as possible, it would "analyze and explain identified discrepancies between component listings and vulnerability scans performed during certification testing." NOAA agreed with the remainder of the recommendations related to this finding.

### **OIG Comments**

We concede NOAA's point that perfect line-by-line consistency between component listings and scans is a difficult task. However, the reasons NOAA provided really describe two scenarios where the scans would not identify components included in the



system security plan. Our review also found the opposite: scans identified components that were not included in the security plan, thus drawing into question the completeness of the system description. This is important because it raises the possibility that other required testing (beyond vulnerability scanning) will not be performed on devices omitted from the security plan, but which are, in fact, a part of the system. That said, we are satisfied with NOAA's intention to analyze and explain discrepancies between scans and component listings, so long as the outcome achieves an accurate depiction of the system and leads to comprehensive certification testing.

## II. Security Control Assessments Were Not Sufficient for Effective Certification

NOAA did not comprehensively scan the components of its systems or properly analyze the results of scans. Unknown vulnerabilities likely exist while those identified were not properly evaluated for possible corrective actions. NOAA also did not perform adequate assessments of management, operational, and technical security controls. As a result, authorizing officials lacked sufficient information for making sound accreditation decisions.

### A. Vulnerability Scanning Was Incomplete and Ineffective

Vulnerability scans of both the POES and SARSAT systems failed to examine many network components. The Seattle LAN was extensively scanned, but vulnerabilities were not analyzed prior to accreditation.

Scanning of POES was limited to only four components, but the C&A package did not explain why. In follow-up discussions with NESDIS's IT security officer, we learned the certification team had not attempted to correct issues that limited scanning. No components residing on the operational network were scanned. Four components were successfully scanned on the development network, but 10 others were not.

The SARSAT C&A package did not define the scope of scanning and provided only a summary of results. Our discussions with NOAA revealed that only workstations and servers were scanned, not firewalls, routers, or switches—key components that provide essential security services. The scans performed were analyzed and documented in the risk assessments, but since not all network components were scanned, unknown vulnerabilities likely exist.

#### Additional scanning of POES and SARSAT also was inadequate

After we discussed our findings that certification scanning was incomplete, NOAA acknowledged the problem and conducted additional scanning on POES and SARSAT. Unfortunately, the additional POES scans were incomplete as well. None of the network components located at NOAA's Fairbanks or Wallops installations were scanned. At NOAA's Satellite Operations Control Center in Suitland, Maryland, only the operational network components within three of seven subnets<sup>5</sup> were scanned.

Additional SARSAT scans included all network components except the five remote local user terminal<sup>6</sup> subnets located in Hawaii, Guam, California, Florida, and Alaska. According to NOAA officials, these subnets were not tested because they could not be scanned remotely, and the certification test team would have to conduct the vulnerability scanning on-site.

---

<sup>5</sup> A subnet is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network.

<sup>6</sup> Local user terminals receive 406 MHz distress signals detected by satellites.

NOAA officials said they made a risk-based decision that scanning the remote subnets would not be cost effective, but that was not explained in the C&A package, and this lack of vulnerability scanning was not identified as a remaining vulnerability to the authorizing official. Because SARSAT is a high impact system, NOAA should develop a strategy to scan all remote network components in future testing.

The results of the additional scans of both POES and SARSAT were not analyzed or addressed in the C&A package, leaving the authorizing official with insufficient information on remaining vulnerabilities.

NOAA's primary scanning tool was unable to evaluate many of the network components

NOAA requires vulnerability scanning to be done using a particular scanning tool that did not consistently complete testing. The scanning tool identified 140 network components of the Seattle LAN, but only 63 were successfully scanned; so more than 50 percent of the network components could not be fully assessed for vulnerabilities. As previously noted, POES vulnerability scanning could only assess 4 of the 14 components on its development network during certification testing. NOAA did not provide information regarding the tool's success rate scanning SARSAT.

We also noted this irregularity in the quarterly vulnerability scans performed on NOAA systems during our FY 2005 assessment of annual testing of security controls. For example, we found that for the National Centers for Coastal Ocean Science Headquarters Support System, the scanning tool identified 237 network components but only 122 were fully scanned. Vulnerability scanning of all network components is necessary to identify and eliminate vulnerabilities.

If NOAA's scanning tool cannot scan all network components of a system, other scanning tools should be used to ensure complete coverage. Department policy and NIST SP 800-42, *Guideline on Network Security Testing*, recommend that more than one scanning tool be used as a matter of practice, since no one scanner can reliably detect all vulnerabilities.

Potentially serious vulnerabilities on the Seattle LAN were not analyzed or corrected

NOAA did use an additional scanning tool and a tool that identifies web application vulnerabilities on the Seattle LAN to supplement its primary tool. The additional tools provided more thorough testing. (See Table 2 for the total number of vulnerabilities found by each scanning tool.) However, the Seattle LAN's C&A package noted that medium and low risk vulnerabilities detected by the primary and supplementary scanning tools were considered acceptable and required no further analysis or mitigation. Only high risk vulnerabilities required evaluation and possible mitigation. However, high risk vulnerabilities were not evaluated or corrected prior to the accreditation decision, and they were not identified to the authorizing official as remaining vulnerabilities.

**Table 2. Number of Vulnerabilities Identified by Risk Level and Scanning Tool (Seattle LAN)**

	<i>High</i>	<i>Medium</i>	<i>Low</i>
<b>Primary Scanning Tool</b>	<b>0</b>	<b>107</b>	<b>149</b>
<b>Supplementary Scanning Tool</b>	<b>59</b>	<b>218</b>	<b>79</b>
<b>Web Application Scanning Tool</b>	<b>8</b>	<b>35</b>	<b>677</b>

Documentation for NOAA’s primary scanning tool states that medium vulnerabilities “provide access to sensitive data” and low vulnerabilities “may be used for information gathering...which could lead to higher risk levels.” Also, the supplementary scanning tool’s documentation states that medium vulnerabilities “are serious security threats that would allow a trusted but non-privileged user to assume complete control of a host, or would permit an untrusted user to disrupt service or gain access to sensitive information,” and low vulnerabilities “may provide an attacker with information that could be combined with other, higher-risk vulnerabilities, in order to compromise the host or its users.”

The Seattle LAN’s C&A package provided a brief analysis of vulnerabilities reported by the supplementary web application scanning tool and says the information was provided to the system administrators to determine resolution and possible mitigation. The vulnerabilities were not corrected prior to the accreditation decision, but they were included in the Plan of Action and Milestone (POA&M) that covered all risks accepted by the authorizing official. However, the POA&M entries were not sufficient to adequately describe the nature of the risks discovered by the scans—something that would be more appropriately documented in the security assessment report.

*Required penetration testing was not performed on POES and SARSAT*

NOAA officials stated that penetration testing, required by Department policy for high-impact systems, would be completed as part of the certification and accreditation process, But neither the POES nor SARSAT systems had penetration tests prior to accreditation. NIST SP 800-42 states that penetration testing is important because it can provide an indication of how vulnerable an organization’s network is and the level of damage that can result if the network is compromised.

In late September 2005, about 3 months after accreditation, NOAA provided OIG with a draft penetration test report for POES. A discussion with the NESDIS IT security officer confirmed our conclusion that only simple vulnerability scanning had been performed, since the report provided no evidence of any attempts to exploit vulnerabilities.

## ***B. Security Control Assessments Did Not Provide Evidence of Effective Management, Operational, and Technical Controls***

POES, SARSAT, and the Seattle LAN control assessments were incomplete, covering only a subset of the minimum security controls described in NIST guidance. Generally, the C&A packages did not include specific procedures for evaluating the controls or adequate documentation of the results. We reviewed the assessments of management and operational controls, but focused on technical control assessments.

### *Ineffective SARSAT and POES control assessments*

Security control assessments considered only a subset of minimum required controls from NIST SP 800-53 or 800-26, but included some additional controls specified by NOAA's IT security office. However, the combined number of management, operational, and technical controls evaluated was less than 66 percent of the controls specified in either NIST SP 800-53 or 800-26, and the majority of those assessed were technical controls, with little attention to management and operational controls.

The procedures used to verify the effectiveness of controls were not defined in more than 60 percent of the assessment cases. And assessment results lacked enough detail to gauge the adequacy of control testing or the effectiveness of the controls.

SARSAT's technical control assessment was barely adequate for certification and unknown vulnerabilities that could be exploited may exist. Only a small sample of network components was evaluated, but the sample did include the primary domain controller that enforces security policy for a significant portion of the system. NOAA assessed the technical controls on 10 of 82 Windows network components and 1 of 8 firewall device components. Servers and workstations within SARSAT run 9 variants, or types, of Windows operating systems. However, components for which technical controls were assessed ran only 4 of these 9 Windows operating system types.,

Controls in routers and switches were not examined. And multiple modems located within the secure boundary—which are access points into the system—were not tested for authentication and session security. These controls would normally enforce the Department policy that passwords and data must be encrypted when transmitted over the Internet or via dial-up connections.

Results of control assessments were provided in SARSAT's C&A package, but some were incomplete or did not include enough information to determine completeness. For example, some controls were identified as "passed" without providing specific results. Others were identified as "failed," but only included results from some of the procedures (multiple procedures are sometimes required to assess a single control).

POES technical control assessment applied the same approach used by SARSAT and was likewise inadequate. Technical control testing was done on only 10 of the 81 Windows network components, and it was unclear if the 4 variants of the Windows operating

systems were tested. As previously mentioned, the lack of unique names for POES network components made it impossible to know which network components were actually tested. In addition, no routers or switches were tested.

#### Minimal Seattle LAN control assessment

The security control assessment of the Seattle LAN evaluated only a subset of the management, operational, and technical controls required by NIST SP 800-53 for a moderate-impact system. The C&A package included little information about assessment activities, and no assessment procedures were defined for any of the controls. Only 22 percent of the controls were identified as assessed, and the results were not provided. Instead, there was only an indication that a given control existed.

NOAA also did not evaluate a sufficient number of components for effective technical controls assessment. The Seattle LAN system inventory identifies 8 servers running 3 variants of the Windows operating system, 128 workstations and laptops running 3 variants of the Windows operating system, 2 variants of the Macintosh operating system, and 1 Linux operating system. However, only 2 network components—a single server and workstation—of the 136 servers and workstations were tested, and no technical control assessment was done on routers or switches. However, the server evaluated was the primary domain controller, which provides essential security services for the network.

#### Comprehensive approach needed to select components for technical control assessments

The approach used to select network components for SARSAT, POES, and the Seattle LAN did not provide for complete testing of all operating system variants running on the servers, workstations, laptops, routers, and switches.

C&A packages for both SARSAT and POES noted that a representative sample of network components had been selected for certification testing. However, 5 of 9 operating system variants were not tested for SARSAT, and it was unclear which variants were not tested for POES.

Seven of nine operating system variants running on the Seattle LAN were not tested. Consequently, the effectiveness of the technical controls operating on the network components of these systems was unknown at the time of accreditation.

Because of technical differences in operating system variants, each should be tested to ensure that technical controls are implemented correctly and operating as intended. A sampling approach would be effective in cases where multiple network components run the same operating system and where each component's operating system is identically configured. In that case, the certification agent should ensure that each uniquely configured operating system variant is tested and provide the rationale for component selection in the C&A package.

### **Recommendations**

The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions:

1. Ensure comprehensive vulnerability scanning.
  - a. Determine whether NOAA's primary network scanner is capable of scanning all network components.
  - b. If not, utilize an additional scanner to permit complete scanning.
2. Analyze and document vulnerability scan results, and take action to correct vulnerabilities.
3. Develop and implement a plan and schedule for conducting penetration testing on all high-impact systems.
4. Comprehensively test management, operational, and technical controls. Develop procedures to evaluate the controls and document test results.
5. Perform technical control tests on components of each uniquely configured operating system variant.
6. Clearly document remaining vulnerabilities in every system so authorizing officials can make credible risk-based decisions on whether or not to accredit the system.

### **NOAA's Response**

NOAA recommended one factual change pertaining to the vulnerabilities discovered by scans of the Seattle LAN. The bureau suggested we change one sentence to reflect the fact that the vulnerabilities were addressed on the system's Plan of Action and Milestones (POA&M) "that covered all risks accepted by the authorizing official." It noted that the POA&M entries, "generally stated that vulnerabilities were discovered by scanners and needed correcting and/or mitigating."

NOAA took exception with our recommendation pertaining to the sampling approach used to test systems (number 5 above), based on the bureau's interpretation of the recommendation to be more exhaustive than we had intended. The bureau suggested we change the wording of the recommendation by replacing the word "identically" with "uniquely." NOAA agreed with the remaining recommendations.

### **OIG Comments**

In regards to the scan results for the Seattle LAN, we have changed the sentence (now on page 12) according to NOAA's suggestion. However, we have also added a sentence indicating that the POA&M entries, which were general statements that vulnerabilities

were discovered by scans, were not sufficient to describe the nature of the risks found by the scans and that such is more appropriately described in the security assessment report.

With respect to our recommendation pertaining to the sampling approach used to test systems, we have changed the wording according to NOAA's suggestion.



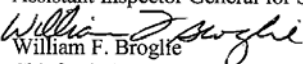
APPENDIX: NOAA'S RESPONSE



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

SEP 12 2006

MEMORANDUM FOR: Judith J. Gordon  
Assistant Inspector General for Systems Evaluation

FROM:   
William F. Broglie  
Chief Administrative Officer

SUBJECT: NOAA's Comments to the Office of Inspector General's  
(OIG) Draft Report—*Progress Being Made in Certification  
and Accreditation Process, but Authorizing Officials Still  
Lack Adequate Decision-making Information*  
Draft Inspection Report No. OSE-18019/August 2006

Thank you for the opportunity to comment on the OIG draft inspection report on information technology certification and accreditation. Attached are the comments from the National Oceanic and Atmospheric Administration.

Attachment



**NOAA's Comments on the Draft OIG Report Entitled  
"National Oceanic and Atmospheric Administration: Progress Being Made in  
Certification and Accreditation Process, but Authorizing Officials Still Lack Adequate  
Decision-making Information"  
(Draft Inspection Report No. OSE-18019/August 2006)**

**General Comments**

The National Oceanic and Atmospheric Administration (NOAA) appreciates the opportunity to comment on the above-mentioned Office of Inspector General (OIG) draft report and looks forward to OIG feedback on recently submitted certification and accreditation (C&A) packages that we believe demonstrate our progress in meeting the recommendations contained in the draft report.

It is important to note that the C&A activities for NOAA 5023 (Search and Rescue Satellite-aided Tracking (SARSAT)) and NOAA 5026 (Polar Orbiting Operational Environmental Satellite Ground System (POES)) began in February 2005, nearly 18 months before issuance of the draft report, and were completed nearly 14 months ago (June 2005).

The observations and recommendations contained in the draft report echo the information provided during the December 2005 OIG exit briefing. NOAA made immediate changes in its C&A process based upon the December 2005 feedback and has also fully adopted guidance in National Institute of Standards and Technology Special Publications 800-53, 800-53A and 800-18, Revision 1. NOAA implemented enhanced internal review processes to ensure completeness and accuracy in all C&A packages, added C&A support staff, and increased the risk analysis and reporting requirements. The NOAA Deputy Under Secretary and the NOAA Chief Information Officer worked with NOAA line office leadership to raise awareness of the resources required to implement and maintain an effective and compliant C&A program. Accordingly, we believe we have implemented most of the recommendations included in the OIG draft report and, as indicated in our responses (below), will continue to take the steps necessary to ensure program effectiveness.

**Recommended Changes for Factual/Technical Information**

*Page 11, second paragraph, second sentence:*

We recommend the sentence read: "However, the vulnerabilities were not corrected prior to the accreditation decision, but they were included in the Plan of Action and Milestone (POA&M) that covered all risks accepted by the authorizing official."

Discussion: The vulnerabilities identified by the vulnerability scanners were documented in the NOAA 6702 POA&Ms, and provided to the authorizing official in the C&A package. The specific POA&Ms include National Ocean Service (NOS) 05.6702.19, NOS 05.6702.20, and NOS 05.6702.21, which generally stated that vulnerabilities were discovered by scanners and needed correcting and/or mitigating.

## NOAA Response to OIG Recommendations

Page 8:

**Recommendation 1a:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions for all C&A packages: Ensure the security plans provide a complete and accurate account of system components. Component listings should be comprehensive and consistent with results of network scanning performed during certification testing.

**NOAA Response:** We agree security plans should provide a complete and accurate account of system components and component listings should be comprehensive. However, perfect line-by-line consistency between a vulnerability scan and the component listing, while desirable, is seldom achievable in a given system for the following reasons:

- If a device in the inventory is old or unique, it may be unknown to the vulnerability scanner software. Examples include Okidata printers, Sun Thin clients, Digital Equipment Corporation (DEC) VAX computers, Macintosh OS 9 and previous, and Sonic Firewalls.
- A device in the inventory may be unavailable due to maintenance or removal from the system during the scan. An example of this is a laptop that is taken on travel.

While perfect line-by-line consistency is seldom achievable, to ensure vulnerability scanning is as thorough and comprehensive as possible, we will analyze and explain identified discrepancies between component listings and vulnerability scans performed during certification testing.

**Recommendation 1b:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions for all C&A packages: Ensure the security plans provide a complete and accurate account of system components. Network topology diagrams should include all key components and be consistent with network scan results.

**NOAA Response:** We concur with the recommendation and will continue to hold appropriate management officials accountable for ensuring security plans and network topology diagrams are complete and accurate.

**Recommendation 1c:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions for all C&A packages: Ensure the security plans provide a complete and accurate account of system components. Components should be uniquely identified so that certification activities can be accurately performed and tracked.

**NOAA Response:** We concur with the recommendation and will continue to hold appropriate management officials accountable for ensuring that uniquely identified system components are included in security plans. This tracking will be accomplished through the review of established C&A schedules and submitted C&A packages.

**Recommendation 2:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions for all C&A packages: Ensure interconnection agreements or memoranda of understandings are obtained and included in future C&A packages.

**NOAA Response:** We concur with the recommendation and will ensure that interconnection agreements or memoranda of understanding are included in future C&A packages.

**Recommendation 3:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions for all C&A packages: Ensure risk assessments are used to tailor security control baselines and provide analysis and justifications for resource-intensive changes to the security features of the information system.

**NOAA Response:** We concur with the recommendation and will continue to ensure that risk assessments are used to tailor security control baselines and provide analysis and justification for changes to system security features.

*Page 14:*

**Recommendation 4:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions: Ensure comprehensive vulnerability scanning, *[including]*:

- a. Determine whether NOAA's primary network scanner is capable of scanning all network components;
- b. If not, utilize an additional scanner to permit complete scanning.

**NOAA Response:** We concur and will perform an analysis to determine whether current network scanning capabilities are sufficient or whether additional scanner(s) are needed for complete scanning.

**Recommendation 5:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions: Analyze and document vulnerability scan results, and take action to correct vulnerabilities.

**NOAA Response:** We concur with the recommendation and will continue to analyze and document vulnerability scan results and correct identified vulnerabilities.

**Recommendation 6:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions: Develop and implement a plan and schedule for conducting penetration testing on all high-impact systems.

**NOAA Response:** We concur with the recommendation and will develop and implement a plan and schedule for performing penetration testing on all high-impact systems.

**Recommendation 7:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions: Comprehensively test management, operation, and technical controls. Develop procedures to evaluate the controls and document test results.

**NOAA Response:** We concur with the recommendation and will continue to refine procedures for evaluating controls and documenting test results. This will be accomplished through security tests and evaluations, as part of the C&A process.

**Recommendation 8:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions: Perform technical control tests on components of each identically configured operating system variant.

**NOAA Response:** We do not concur with the recommendation as written. We agree with the goal of comprehensively testing systems. However, we believe that if systems are under configuration management and are identically configured, it is unnecessary and costly to test all identical systems. A statistical testing approach of a significant representative sample should be reasonable testing where similarly configured systems are under configuration management. Therefore, we believe that the recommendation should read: *“Perform technical control tests on components of each uniquely configured operating system variant.”*

**Recommendation 9:** The Deputy Undersecretary for Oceans and Atmosphere should direct appropriate management officials to take the following actions: Clearly document remaining vulnerabilities in every system so authorizing officials can make credible risk-based decisions on whether or not to accredit the system.

**NOAA Response:** We concur with the recommendation and will ensure that system vulnerabilities are clearly documented and presented to the authorizing official.



U.S. DEPARTMENT OF COMMERCE  
Office of Inspector General

Room 7099C, HCHB  
1401 Constitution Avenue, N.W.  
Washington, D.C. 20230

Internet Web Site:  
[www.oig.doc.gov](http://www.oig.doc.gov)

CULTIVATE  
PEACE AND  
COMMERCE  
WITH ALL  
JEFFERSON