



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



***National Oceanic and
Atmospheric Administration***

***FY 2008 FISMA Assessment of
National Weather Service
Telecommunication Gateway
(NOAA8871)***

Final Inspection Report No. OSE-19000/September 2008

FOR PUBLIC RELEASE

Office of Systems Evaluation



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

SEP 22 2008

MEMORANDUM FOR: Vice Admiral Conrad C. Lautenbacher, Jr., USN (Ret.)
Under Secretary of Commerce for Oceans and Atmosphere
and NOAA Administrator

Mary M. Glackin
Deputy Under Secretary of Commerce for Oceans and
Atmosphere

FROM: Judith J. Gordon
Assistant Inspector General for Audit and Evaluation

SUBJECT: National Weather Service
*FY 2008 FISMA Assessment of NWS Telecommunication
Gateway (NOAA8871)*
Final Inspection Report No. OSE-19000

This report presents the results of our Federal Information Security Management Act (FISMA) review of the certification and accreditation of the NWS Telecommunication Gateway system. We found that the system security plan did not provide an adequate basis to conduct the security certification and NWS needs to improve its security control assessments to assure that controls are implemented correctly and operating as intended.

In response to our draft report, NOAA, with one exception, agreed with our findings and described corrective actions that are fully responsive to all our recommendations. NOAA's response is summarized in the appropriate sections of the report and included in its entirety as appendix B.



We request that you provide us an action plan describing the actions you have taken or plan to take in response to our recommendations within 60 calendar days of the date of this report. The plan should be in the form of plans of action and milestones (POA&Ms) 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) 482-2754 or Allen Crawley, Deputy Assistant Inspector General for Systems Evaluation at (202) 482-1855.

Attachment

cc: Suzanne Hilding, Chief Information Officer, U.S. Department of Commerce
Joe Klimavicz, Chief Information Officer, National Oceanic and Atmospheric
Administration
Dr. Jack L. Hayes, Assistant Administrator for Weather Services, National Weather
Service
Adrian R. Gardner, Chief Information Officer, National Weather Service

Listing of Abbreviated Terms & Acronyms

C&A	Certification and Accreditation
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
	
IP	Internet Protocol
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NWS	National Weather Service
NWSTG	National Weather Service Telecommunication Gateway
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RPC	Remote Procedure Call
SAR	Security Assessment Report
SSP	System Security Plan
ST&E	Security Testing and Evaluation
TOC	Telecommunication Operations Center

Synopsis of Findings

- Security controls were not adequately defined prior to the certification phase or in the approved system security plan.
- Secure configuration settings were not defined for some IT products and none were assessed.
- Certification assessments were incomplete and flawed.
- OIG assessment of selected security controls found significant weaknesses not identified by the NWS security certification.

Conclusion

- NWS needs to improve security control assessments to assure that controls are implemented correctly, operating as intended, and meeting the security requirements for the system.

Summary of NOAA Response

In its response to our draft report, NOAA, with one exception, agreed with our findings. NOAA noted that, although the SSP was not signed when certification testing began, it had been favorably reviewed by NWS' information technology security officer and the system's authorizing official.

Also, NOAA concurred with all our recommendations and identified actions it will take to address them. These actions include the remediation of specific vulnerabilities, reassessments of security control implementations, updates to security requirements, and changes to hiring processes, security training, and C&A contract requirements.

NOAA's written response is included in its entirety as appendix B of this report.

OIG Comments

NOAA's response took exception with the first finding that stated the security certification began before the SSP was formally reviewed and approved. Although NOAA asserts that the authorizing official and NWS' senior IT security officer had reviewed the SSP before beginning security certification, the SSP was not approved until after the accreditation decision. Department policy and NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, require approval of the SSP by the authorizing official and senior agency information security officer to ensure the set of security controls specified in the SSP meet the security requirements for the information system before advancing to the security certification phase.

The corrective actions described by NOAA are responsive to our recommendations.

Introduction

The National Weather Service Telecommunication Gateway (NWSTG) supports the National Weather Service's (NWS') mission to collect, process, and disseminate national and international meteorological data and products in real time. Other governmental agencies, the private sector, the general public, and the global community also use the system's data.

NWS has categorized NWSTG [REDACTED] system, which means that a security breach could be expected to have [REDACTED] effect on organizational operations, organizational assets, or individuals.

The system interconnects with numerous other systems worldwide via various protocols. Network components (primarily [REDACTED] firewalls, routers, and switches) regulate the flow of internal and external communications. The system comprises [REDACTED], and Windows servers that gather, process, and disseminate meteorological information and manage the system infrastructure. Workstations are used for interacting with and monitoring the system. Key applications in the system include databases and Web servers.

Findings and Recommendations

1. Security Controls Were Not Adequately Defined Prior to the Certification Phase or in the Approved System Security Plan

- NWS began the security certification before the security controls were adequately defined and the SSP was formally reviewed and approved, resulting in an ineffective C&A process.
 - According to the SAR, certification assessments began around March 2, 2007 but the SSP was not approved until the system was accredited on March 22, 2007.
- The SSP did not adequately define the control enhancements required for [REDACTED] system or the organization-defined security control parameters. It also mistakenly identified controls as NOAA common controls. *(The following totals do not include organization-defined parameters and security control enhancements identified as planned or controls accurately identified as NOAA common controls.)*
 - The SSP did not define 24 of [REDACTED] security control enhancements required for a [REDACTED] impact system.
 - AC-17 [REDACTED] – Remote Access
 - AU-2 [REDACTED] – Auditable Events
 - CM-2 [REDACTED] – Baseline Configuration
 - CM-3 [REDACTED] – Configuration Change Control
 - CP-2 [REDACTED] – Contingency Plan
 - CP-3 [REDACTED] – Contingency Training
 - CP-4 [REDACTED] – Contingency Plan Testing
 - CP-6 [REDACTED] – Alternate Storage Sites
 - CP-7 [REDACTED] – Alternate Processing Sites
 - CP-8 [REDACTED] – Telecommunications Services
 - CP-9 [REDACTED] – Information System Backup
 - MA-2 [REDACTED] – Controlled Maintenance
 - MA-4 [REDACTED] – Remote Maintenance
 - Eight of [REDACTED] organization-defined security control parameters for tailoring the control baseline were not defined.
 - AU-5 – Percentage of maximum audit record storage capacity permitted before information system takes appropriate actions
 - AU-6 – List of inappropriate or unusual activities that result in alerts
 - CM-7 – List of prohibited and/or restricted functions, ports, protocols, and/or services
 - CP-7 – Time period by which critical mission functions at the alternate site must be resumed
 - CP-8 – Time period by which telecommunications services must be resumed
 - CP-9 – Frequency of testing for backup media to verify reliability and integrity
 - PE-8 – Frequency of visitor access records review by designated organization officials
 - RA-5 – Frequency of updates of list of scanned information security vulnerabilities

- Ten of 19 physical and environmental controls were incorrectly identified as NOAA common controls.
 - PE-8 – Access Records
 - PE-9 – Power Equipment and Power Cabling
 - PE-10 – Emergency Shutoff
 - PE-11 – Emergency Power
 - PE-12 – Emergency Lighting
 - PE-13 – Fire Protection
 - PE-14 – Temperature and Humidity Controls
 - PE-15 – Water Damage Protection
 - PE-16 – Delivery and Removal
 - PE-18 – Location of Information System Components
- Impacts of inadequately defined security controls include:
 - Controls may not have been completely or accurately implemented by the system owner.
 - Certification team lacked information to effectively assess the control.
 - Assessments of physical and environmental controls were incomplete.

Recommendation

- 1.1 NOAA should ensure that the authorizing official and senior information security officer review and approve the system security plan prior to certification. The system information should be accurate and proposed security controls should meet the system's security requirements. Approval should confirm that the SSP
- correctly identifies security controls not directly supervised by the system owner,
 - adequately describes all applicable required control enhancements, and
 - specifies all security control parameters required to be defined by the organization.

2. Secure Configuration Settings Were Not Defined for Some IT Products and None Were Assessed

Background: The Department's IT security policy and NIST SP 800-53 require establishing and assessing secure configuration settings for IT products. Products include operating systems for system components (such as servers, desktops, laptops, routers, and switches) and applications (such as e-mail, Web, VPN, firewall, intrusion detection, database, and antivirus). FISMA and OMB guidance also highlight the importance of secure configuration settings. Implementing and maintaining secure configuration settings is one of the most effective ways of negating threats. Failing to completely assess this critical control leaves the security of a system in serious doubt and undermines the adequacy of the certification.

- Secure configuration settings were defined only for Windows, [REDACTED] IT products.
 - Settings were not defined for the following:
 - [REDACTED] routers, switches, and firewalls
 - [REDACTED] Web server
 - [REDACTED] server
- No secure configuration settings were assessed.
 - The package contained no evidence that secure configuration settings had been evaluated for any IT product.
 - The certification team inappropriately assessed the control by relying on a statement from the system security officer who stated, "Configuration settings have been set to the most restrictive modes and enforced on all components in the NWSTG."
 - During our field work, NWS claimed secure configuration settings had been assessed both with an automated scanning tool and manually. However, we found
 - The scanning tool used could not have assessed the control since it was not configured to evaluate NWS' secure configuration baselines.
 - The certification team could not provide any evidence of manual assessments.

Recommendations

NOAA should ensure that

- 2.1 secure configuration settings are defined and implemented for all IT products in the system accreditation boundary in accordance with NIST SP 800-70, *Security Configuration Checklists Program for IT Products*; and
- 2.2 a sample of identically configured components running each operating system variant is assessed for compliance with organizationally defined operating system baselines and appropriate samples of other IT products.

3. Certification Assessments Were Incomplete and Flawed

- C&A package lacks evidence that security controls were assessed on all applicable system components and applications where the controls are implemented.
 - Network devices including [REDACTED] routers, firewalls, switches, and [REDACTED] switches and applications including [REDACTED] were not assessed.
 - Not all applicable operating systems were assessed for some security controls. (See table 1 for examples.)
 - The majority of the artifacts referred to in the procedural step assessment results are for [REDACTED]. Minimal artifacts exist to support control assessments on Windows and [REDACTED]
 - OIG determinations were based on reviewing the procedural step assessment results and artifacts. Because some results and artifacts were insufficient to determine if the control was assessed on all applicable system components, we considered any other associated results and artifacts not directly related to the procedural step.
- Certification assessment results erroneously indicated that some procedural steps for control assessments were related to NOAA common controls. As a result, the following assessments were not performed during certification:
 - Individual procedural steps:
 - AC-4.2 – Information Flow Enforcement – Information flow within the system and between systems
 - SI-2.7 – Flaw Remediation – Test effectiveness of flaw remediation capabilities
 - SA-7.3 – User Installed Software – Examine firewall logs for indications of prohibited software
 - All the procedural steps for the following controls:
 - AT-3 – Security Training
 - PE-3 – Physical Access Control
 - PE-4 – Access Control for Transmission Medium
 - PE-5 – Access Control for Display Medium
 - PE-6 – Monitoring Physical Access
 - PE-7 – Visitor Control
 - PE-17 – Alternate Work Site
- Four security controls that should have been assessed on system components inappropriately relied on interviews and document review. (See table 2.)
- Some security control assessments did not follow procedures and contained results inconsistent with evidence. (See table 3 for examples.)
- Some certification assessment results did not describe vulnerabilities discovered. (See table 4 for examples.)
 - Assessment results indicated only “POA&M” with no further explanation.
 - If vulnerabilities are not identified and described, officials cannot be certain of
 - the specific deficiencies within the control,
 - the amount of risk that should be attributed to the system from the failed control assessment, and
 - how to mitigate the vulnerabilities.

Recommendations

NOAA should ensure that

- 3.1 security controls are assessed on all applicable system components, such as routers, switches, firewalls, applications, and servers;
- 3.2 control assessments follow applicable procedures; and
- 3.3 assessment results clearly describe vulnerabilities discovered.

Table 1: Examples of Assessments Not Performed on All Applicable Operating Systems.

Certification Test Results from Certification Documentation Package		OIG Determination of Assessment on Applicable Operating Systems		
Procedural Step	Certification Test Results (full quotation)	Windows [REDACTED]	[REDACTED]	[REDACTED]
AC-2.20 Test selected automated mechanisms within the information system that support the account management auditing and notification functions to determine if: (i) the mechanisms are operating as intended; (ii) each of the account actions identified produce accurate and informative audit records; and (iii) each action, as required by the account management procedures, results in notification of appropriate individuals.	[REDACTED]	Assessed – We determined the control was assessed on Windows using the Nessus policy scanner.	Not Assessed – The artifacts do not relate to the procedural step.	Not Assessed
AC-7.2 Examine the information system configuration settings to determine if the information system enforces organizational policy and procedures for unsuccessful login attempts.	[REDACTED]	Assessed – We determined the control was assessed on Windows using the Nessus policy scanner.	Assessed – We determined that the control was assessed using the results from AC-7.3.	Not Assessed

Table 1: Examples of Assessments Not Performed on All Applicable Operating Systems.

Certification Test Results from Certification Documentation Package		OIG Determination of Assessment on Applicable Operating Systems		
Procedural Step	Certification Test Results (full quotation)	Windows		
<p>AC-11.3 Test the session lock mechanism by allowing a user session to remain inactive for the organization-defined period to determine if the session lock automatically occurs on the information system and that the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.</p>	<p>[REDACTED]</p>	<p>Not Assessed</p>	<p>Not Assessed – The test result artifact is not applicable because it only shows unsuccessful login attempts. No other artifacts indicate this control was assessed.</p>	<p>Not Assessed</p>
<p>AU-2.1 Examine organizational records or documents and the information system configuration settings to determine if the system generates audit records for the organization-defined auditable events</p>	<p>[REDACTED]</p>	<p>Assessed – The test result does not indicate that Windows servers were assessed; however, we determined that the control was assessed on Windows using the Nessus policy scanner.</p>	<p>Assessed – The test result does not indicate that [REDACTED] were assessed. However, artifact AU-01 [REDACTED] contains configuration data indicating the control was assessed.</p>	<p>Not Assessed</p>

Table 1: Examples of Assessments Not Performed on All Applicable Operating Systems.

Certification Test Results from Certification Documentation Package		OIG Determination of Assessment on Applicable Operating Systems		
Procedural Step	Certification Test Results (full quotation)	Windows [REDACTED]	[REDACTED]	[REDACTED]
AU-4.1 Examine the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded.	[REDACTED]	Assessed – We determined the control was assessed on Windows using the Nessus policy scanner.	Not Assessed	Not Assessed
IA-2.6 Test the appropriate components within the information system to determine if passwords, tokens, or biometrics meet Level 3 or 4 requirements consistent with NIST Special Publication 800-63.	[REDACTED]	Assessed – We determined the control was assessed on Windows using the Nessus vulnerability scanner.	Assessed – Supported by artifact	Not Assessed

Table 1: Examples of Assessments Not Performed on All Applicable Operating Systems.

Certification Test Results from Certification Documentation Package		OIG Determination of Assessment on Applicable Operating Systems		
Procedural Step	Certification Test Results (full quotation)	Windows	Linux	Other
SC-10.2 Test the network disconnection capability for the information system by leaving an open session for a specified amount of time to determine if the system terminates the network connection as expected.	[REDACTED]	Not Assessed	Assessed – Supported by artifact	Not Assessed

Table 2: Assessments that Inappropriately Relied on Documentation and Interviews

Control	Procedural Step	Certification Test Results (full quotation)	OIG Comments
AC-2 Account Management	AC-2.3 Examine selected active user accounts to determine if the organization followed procedures to establish and activate the user accounts and complete any organization-required documentation.	[REDACTED]	Results do not indicate whether selected active user accounts on system components were actually examined during certification testing.
CM-6 Configuration Settings	CM-6.2 Examine selected information system configuration settings to determine if they are configured in accordance with the organization-defined settings.	[REDACTED]	Results do not indicate that configuration settings were assessed on any IT products.
CP-9 Information System Backup	CP-9.2 Examine selected information system backup media, or selected records of backups if available, to determine if the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency and stores the backup information in designated locations in accordance with information system backup procedures.	[REDACTED]	Results do not indicate that backup media or records of backups were examined. The results are just a description of how the control is implemented from the SSP.

Table 2: Assessments that Inappropriately Relied on Documentation and Interviews



Control	Procedural Step	Certification Test Results (full quotation)	OIG Comments
			
MA-2 Controlled Maintenance	MA-2.7 Examine the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that periodic maintenance is scheduled and conducted as required.		Results do not indicate that the automated mechanisms within the information system were examined. The results indicate that only the <i>Maintenance Procedures</i> and <i>Patch Procedures</i> documents were reviewed.

Table 3: Examples of Assessments that Did Not Follow Procedural Steps

Control	Procedural Step	Certification Test Results (full quotation)	OIG Comments
AC-2 Account Management	AC-2.20 Test selected automated mechanisms within the information system that support the account management auditing and notification functions to determine if: (i) the mechanisms are operating as intended; (ii) each of the account actions identified produce accurate and informative audit records; and (iii) each action, as required by the account management procedures, results in notification of appropriate individuals.	[REDACTED]	The procedural step to test the auditing and notification of account management functions was not followed. The referenced artifacts do not contain audit records or indicate that account management activity notifications occurred. The artifacts only show that audit log files exist, access to a single directory is restricted, and unsuccessful login attempts are logged.
AC-3 Access Enforcement	AC-3.3 Examine the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations.	[REDACTED]	The procedural step of examining user access rights against documented user authorizations was not followed. The referenced artifact does not show any comparison of user permissions with the documented TOC Access Control Policy, secure configuration baselines, or any other documented user authorizations. The artifact only shows that audit log files exist and access to a single directory is restricted.
AC-5 Separation of Duties	AC-5.3 Examine selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and	[REDACTED]	The procedural step to examine information system accounts to determine if users have the ability to perform conflicting security functions was not followed. The results statement was copied from the SSP and no evidence was provided showing that account authorizations or privileges were assessed. In addition, an interview conducted during certification contained a statement indicating that [REDACTED] We do not have an independent test group or implementation group.

Table 3: Examples of Assessments that Did Not Follow Procedural Steps

Control	Procedural Step	Certification Test Results (full quotation)	OIG Comments
	(iii) security personnel who administer access control functions should not administer audit functions).		In our situation the developers test, and the developers are the environment owners.”
MA-2 Controlled Maintenance	MA-2.8 Examine the log of maintenance actions to determine if the log is up to date, accurate, complete, and available.	[REDACTED]	The procedural step to examine the log of maintenance actions was not followed. The results only define the location of the logs. There is no indication that the logs were examined.
MA-3 Maintenance Tools	MA-3.2 Examine approved information system maintenance tools and associated documentation to determine if the organization maintains the tools and documentation on an ongoing basis and if the processes applied are consistent with the documented maintenance procedures.	[REDACTED]	The procedural step to examine maintenance tools and associated documentation was not followed. The results only define the location of the maintenance tools and documentation. There is no indication that the tools or documentation were examined.
SA-7 User Installed Software	SA-7.5 Test network traffic on the information system to determine if prohibited software is installed and operational by utilizing a network packet analyzer. (Note: Applications tend to communicate on known ports and/or have signature traffic patterns and common packets.)	[REDACTED]	The procedural step to perform network packet analysis was not followed. The C&A package did not contain any evidence of network packet analysis.
SA-7 User Installed Software	SA-7.6 Test the information system for prohibited software by utilizing a scanner which detects and reports the names of installed software; compare the results against the approved software applications	[REDACTED]	The procedural step to detect and report names of installed software and compare the results against approved software applications was not followed. Our evaluation of the scanner results concluded that the scanners did not detect and

Table 3: Examples of Assessments that Did Not Follow Procedural Steps

Control	Procedural Step	Certification Test Results (full quotation)	OIG Comments
	list.		report names of installed software. Also, no evidence was provided showing that installed applications were compared against a list of approved software applications.
SC-14 Public Access Protections	SC-14.2 Test the publicly available information system by attempting to alter protected information using a public account to determine if access is limited in order to preserve the integrity of the information and the applications.	[REDACTED]	NWS was unable to provide evidence that the procedural step to attempt to alter protected information using a public account was followed.
SC-18 Mobile Code	SC-18.2 Test the information system by attempting to run mobile code in an application where it is specifically prohibited to determine if the organization implements mobile code usage restrictions.	[REDACTED]	The procedural step to test applicable information system components by attempting to run mobile code was not followed. The artifact shows attempts to access the Internet from scanning machines that are not within the accreditation boundary. There is also no evidence the procedure was performed on applicable system components with Internet access.

Table 4: Examples of Results that Do Not Clearly Indicate Why the Assessment Failed.

Procedural Step	Expected Result (full quotation)	Actual Results (full quotation)
<p>AC-4.1 Examine information system interconnection agreements to determine if the agreements address: (i) the types of permissible and impermissible flow of information between systems; and (ii) the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.</p>	<p>[REDACTED]</p>	<p>POA&M</p>
<p>MP-2.7 Test the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that media access is restricted as required.</p>	<p>[REDACTED]</p>	<p>POA&M</p>
<p>SC-12.1 Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and management and how the mechanisms and procedures are implemented.</p>	<p>[REDACTED]</p>	<p>POA&M</p>
<p>SC-21.2 Test the information system by attempting to launch known attacks against the domain name servers.</p>	<p>[REDACTED]</p>	<p>POA&M</p>
<p>SI-7.5 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software and information integrity control is implemented.</p>	<p>[REDACTED]</p>	<p>POA&M</p>

Table 5: Comparison of Certification Assessment Results Against OIG Assessment Results

Certification Assessment		OIG Assessment	
Procedural Step	Certification Test Results (full quotation)	IT Product	OIG Assessment Results
<p>AC-2.4 Examine a list of recently disabled information system accounts and compare to selected system-generated records with user IDs and last login date for each account to determine if the last log-in date is beyond the date that the account is disabled.</p>	<p>[REDACTED]</p>	[REDACTED]	Disabling inactive system accounts is not enforced on one of the five [REDACTED] components. We identified an administrator account not used in more than a year but which was not disabled.
		[REDACTED]	Disabling inactive system accounts is not enforced on either [REDACTED] component. We found four system administrator accounts that had never been used or had been inactive for more than 90 days but had not been disabled.
		[REDACTED]	Disabling inactive system accounts is not enforced on the [REDACTED] database component. We found two accounts that had been inactive for at least 100 days but had not been disabled.
		Windows	Disabling inactive system accounts is not enforced on three of the four Windows components. We identified six accounts that were inactive for at least 1 year or had never been used but had not been disabled.
<p>AC-2.20 Test selected automated mechanisms within the information system that support the account management auditing and notification functions to determine if:</p> <p>(i) the mechanisms are operating as intended; (ii) each of the account actions identified produce accurate and informative audit records; and</p> <p>(iii) each action, as required by the account management procedures, results in notification</p>	<p>[REDACTED]</p>	[REDACTED]	[REDACTED]

Table 5: Comparison of Certification Assessment Results Against OIG Assessment Results

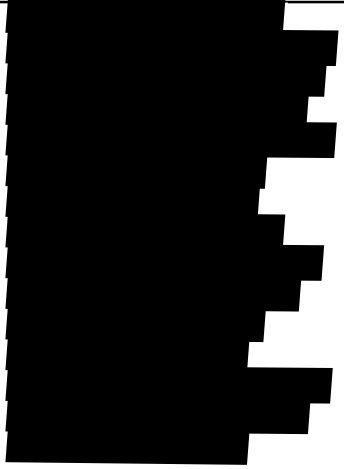
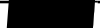


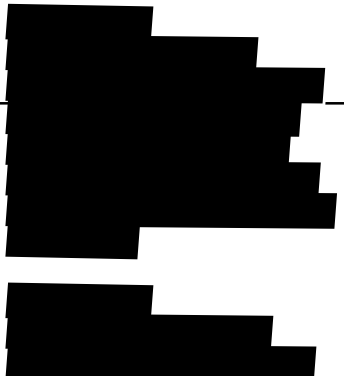




Certification Assessment		OIG Assessment	
Procedural Step	Certification Test Results (full quotation)	IT Product	OIG Assessment Results
of appropriate individuals.			
AC-3.2 Examine access control mechanisms to determine if the information system is configured to implement the organizational access control policy.			
		Windows	
AC-7.3 Test the account lockout policy on selected user accounts by exceeding the maximum number of invalid login attempts within the organization-defined time period on the information system to determine if the information system locks the account/node.			
			
			

Table 5: Comparison of Certification Assessment Results Against OIG Assessment Results

Certification Assessment		OIG Assessment	
Procedural Step	Certification Test Results (full quotation)	IT Product	OIG Assessment Results
			[REDACTED]
		[REDACTED]	[REDACTED]
AC-7.8 Examine the information system configuration settings to determine if the information system is configured to automatically lock the account/nodes until released by the administrator when the maximum number of unsuccessful attempts is exceeded.	[REDACTED]	Windows	[REDACTED]
AU-2.2 Test the information system by attempting to perform actions that are configured to generate an audit record.	[REDACTED]	[REDACTED]	[REDACTED]
		Windows	[REDACTED]
CM-7.2 Test the information system to determine if the identified functions, ports, protocols, and services are prohibited or restricted.	[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		Windows	[REDACTED]

Table 5: Comparison of Certification Assessment Results Against OIG Assessment Results

Certification Assessment		OIG Assessment	
Procedural Step	Certification Test Results (full quotation)	IT Product	OIG Assessment Results
			[REDACTED]
IA-2.3 Test the information system to determine if passwords, tokens, or biometrics meet Level 2, 3, or 4 requirements consistent with NIST Special Publication 800-63.	[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		Windows	[REDACTED]

Table 5: Comparison of Certification Assessment Results Against OIG Assessment Results

Certification Assessment		OIG Assessment	
Procedural Step	Certification Test Results (full quotation)	IT Product	OIG Assessment Results
			[REDACTED]
IA-5.3 Examine organizational records or documents to determine if the organization changes default authenticators upon information system installation.	[REDACTED]	[REDACTED]	[REDACTED]
IA-5.7 Test the information system to determine if the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, enforces password minimum and maximum lifetime restrictions, and prohibits password reuse for a specified number of generations.	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]

Appendix A: Objectives, Scope, and Methodology

To meet the FY 2008 FISMA reporting requirements, we evaluated the NOAA certification and accreditation for the National Weather Service Telecommunication Gateway (NOAA8871).

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 **plan of action & milestones** is based on the results of the security assessment. It documents actions taken or planned to address remaining vulnerabilities in the system.

Commerce'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.
- The **certification test results**, which is the raw data collected during the assessment.

To evaluate the C&A package, we reviewed all components of the package and interviewed NWS staff to clarify any apparent omissions or discrepancies in the documentation and gain further insight on the extent of the security assessment. We give substantial weight to the evidence that supports the rigor of the security assessment when reporting our findings to OMB.

In addition, we performed our own security control assessments on NWSTG and compared our results with NWS' certification test results. We chose a subset of the control requirements specified in NIST SP 800-53, and a subset of assessment procedures from NIST SP 800-53A, Third Public Draft. We tailored the procedures to NWS' specific control implementations. We did not attempt to perform a complete assessment of each control; instead we chose to focus on specific aspects of some of the more important technical and operational controls.

We assessed controls on key classes of IT components and applications, choosing a targeted set of components from each class that would allow for direct comparison with NWS' certification test results. We assessed control implementations on: [REDACTED] components, Windows [REDACTED], [REDACTED] (router/switch/firewall combos), [REDACTED], and a [REDACTED]. In addition, we examined the security plan descriptions, including related policy documents, and interviewed appropriate NWS personnel.

Because NWSTG [REDACTED] security objective, we adapted our assessments to minimize the impact on system operations by assessing standby components when possible. We could not perform some assessments on certain system components. For example, we did not assess the creation, modification, or deletion of user accounts on routers, firewalls,

and switches. Our assessments included the following activities:

- Extraction, examination, and verification of system configurations
- Generation of system events and examination of system logs
- Execution of DISA scripts (Gold Disk)
- Examination of user and group authorizations
- Addition, modification, and deletion of operating system accounts

Our assessment was limited in scope and should not be interpreted as the comprehensive review that a security certification [REDACTED] system would require. However, our assessments gave us direct assurance of the status of select aspects of important controls in NWSTG and provided meaningful comparison to the NWS security certification.

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*
- NIST's 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*
 - 800-42, *Guideline on Network Security Testing*
 - 800-53, *Recommended Security Controls for Federal Information Systems*
 - 800-70, *Security Configuration Checklists Program for IT Products*

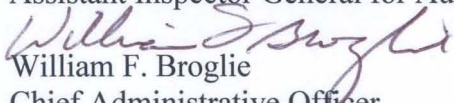
We conducted our evaluation in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency in January 2005.



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

AUG 21 2008

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

FROM: 
William F. Broglie
Chief Administrative Officer

SUBJECT: *FY 2008 FISMA Assessment of NWS Telecommunication Gateway (NOAA8871)*
Draft Inspection Report No. OSE-19000/June 2008

Attached is the National Oceanic and Atmospheric Administration's response to the Office of Inspector General's draft report on its Federal Information Security Management Act review of the National Weather Service Telecommunication Gateway system. The response was prepared in accordance with Department Administrative Order 213-3, *Inspector General Auditing*. We appreciate the opportunity to respond to your draft report.

Attachment



**Department of Commerce
National Oceanic and Atmospheric Administration
Comments on the Draft OIG Report Entitled
“FY 2008 FISMA Assessment of National Weather Service
Telecommunication Gateway (NOAA8871)”
(OSE-19000/June 2008)**

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 Weather Service (NWS) Telecommunication Gateway (NWSTG). Although corrective actions were underway for many of the recommendations and findings in this report, NWS does not dispute those corrective actions were not yet complete when the OIG assessment took place.

Currently, the contractor that conducted the NWSTG certification testing is in the process of redoing that certification testing at no charge to NWS, and is expected to complete re-accreditation of the system by August 29, 2008. NWS has incorporated lessons learned from this OIG assessment in current and future Certification and Accreditation (C&A) activities for high impact systems.

Several corrective actions were underway when the OIG reviewed this system, including the following:

- Key personnel actions have been completed and others are underway to strengthen the computer security protections for this system and other systems across NWS;
- Organizational changes have been made and others are underway to provide better subject matter expertise in the oversight of the NWS C&A program (to include creation of a GS-15 Chief Information Security Officer position within the NWS Office of the Chief Information Officer to oversee all NWS C&A activities);
- Computer security program criteria will be added to the annual performance metrics for Regional Directors and other appropriate personnel; and
- An NWS-wide Information Management Council was established to coordinate C&A processes and knowledge across NWS.

Implementation of additional corrective actions is dependent upon the results of the new NWSTG certification testing.

Recommended Changes for Factual/Technical Information

Page 4, first bullet:

The OIG correctly notes the NWSTG System Security Plan (SSP) was not signed when the certification testing began. However, the NWS Information Technology Security Officer (ITSO) and the Authorizing Official favorably reviewed the SSP before testing commenced.

NOAA Response to OIG Recommendations

Recommendation 1: “1.1 NOAA should ensure that the authorizing official and senior information security officer review and approve the system security plan prior to certification. The system information should be accurate and proposed security controls should meet the system’s security requirements. Approval should confirm that the SSP

- correctly identifies security controls not directly supervised by the system owner,
- adequately describes all applicable required control enhancements, and
- specifies all security control parameters required to be defined by the organization.”

NOAA Response: We concur. NWS is hiring a new System Owner, Information System Security Officer (ISSO), and NWS ITSO and is including as part of the selection process the candidates’ understanding of C&A requirements. As an immediate action, NWS has temporarily assigned a highly-qualified System Owner from another NWS component to oversee the technical corrective actions to address the OIG findings.

NWS is processing an organizational change that will replace the current position of “NWS ITSO” with a new position of NWS Chief Information Security Officer (CISO) at the GS-15 level. Under this organizational change, the new ISSO for NWSTG will report and be accountable to the new NWS CISO.

Information security compliance has been added to the performance appraisal requirements of all NWS senior executives, system owners, and information technology (IT) managers. Information security compliance includes the need to infuse system security into the organizational culture at all levels and to address security needs in budget and resource requirements supporting day-to-day operations.

The SSP is being updated to define all security control enhancements and parameters required for high-impact systems. (Plan of Action and Milestones (POA&M) item: NOAA8871-08.01, Security control enhancement and parameter definition; scheduled completion date 9/30/09)

The SSP will also be updated to match current NOAA common controls. (POA&M item: NOAA8871-08.02, NOAA common control review and update; scheduled completion date 9/30/09)

Recommendation 2: “NOAA should ensure that

2.1 secure configuration settings are defined and implemented for all IT products in the system accreditation boundary in accordance with NIST SP 800-70, *Security Configuration Checklists Program for IT Products*; and

2.2 a sample of identically configured components running each operating system variant is assessed for compliance with organizationally defined operating system baselines and appropriate samples of other IT products.”

NOAA Response: We concur. Through security awareness training and system owner training, NWS will provide system owners and technical staff with greater understanding of threats, vulnerabilities, countermeasures, and C&A compliance strategies and details.

NWS is also developing a strategy to facilitate investment decisions to support the needs of system owners to understand and drive compliance with the confidentiality, availability, and integrity requirements of their systems.

Similarly, contracts and task orders for C&A must include detailed descriptions of the expected deliverables for potential vendors.

At a technical level, NWS secure configuration baselines are being defined and implemented for configurable off-the-shelf software, operating systems, and network devices. (POA&M item: NOAA8871-08.03, scheduled completion date 9/30/09)

As part of the current redo of the certification testing, reassessment of all applied secure configuration baselines is being performed and relevant documentation will be updated to correct the deficiencies from the OIG findings, including maintaining appropriate artifacts, where applicable.

Recommendation 3: “NOAA should ensure that

3.1 security controls are assessed on all applicable system components, such as routers, switches, firewalls, applications, and servers;

3.2 control assessments follow applicable procedures; and

3.3 assessment results clearly describe vulnerabilities discovered.”

NOAA Response: We concur. NWS is examining resource requirements to provide a comprehensive monitoring capability with technical staff and tools that will provide continuous security monitoring of NWS networks, devices, boundaries, and NOAA common controls.

At a technical level, as part of the redo of the certification testing, re-evaluation and correction of procedural steps relating to NOAA common controls are being performed, as is a reassessment of all controls on all applicable system components and software pertaining to a high availability system. Relevant documentation will be updated after the certification testing is completed.

Recommendation 4: “NOAA should ensure that

4.1 the deficiencies we identified are added promptly to the system’s plan of action and milestones, and remediated in a timely manner; and

4.2 control assessments, both for continuous monitoring and future security certifications, include more thorough interviews, examinations, and tests.”

NOAA Response: We concur. At a technical level, NWS is addressing the following:

- Account management policy, procedure, and implementation are being reviewed and modified as necessary. (POA&M item: NOAA8871-08.04, scheduled completion date 9/30/09)
- Audit implementation is being reviewed on all systems and modified as necessary. (POA&M item: NOAA8871-08.04, scheduled completion date 9/30/09)
- Configuration management, including system integrity controls, is being implemented or modified as necessary. (POA&M item NOAA8871-07, scheduled completion date 9/1/08)
- The vendor default password found on a [REDACTED] appliance is not externally accessible due to network protection, but was changed immediately after the initial OIG briefing. Password management settings are currently being reviewed. (POA&M item: NOAA8871-07.02, scheduled completion date 9/1/08)
- Identification and baseline configuration of the anti-virus application is currently underway. (POA&M item: NOAA8871-07.02, scheduled completion date 9/1/08)

Appendix C: Assessment of Selected Security Controls

A compact disk containing the procedures we used to assess security controls implemented on selected system components from the Telecommunication Gateway system was provided to NWS. The disk also included our assessment results, analysis, and supporting evidence.

