



U.S. DEPARTMENT OF COMMERCE
Office of Inspector General



***National Institute of Standards
and Technology***

***FY 2009 FISMA Assessment of
Manufacturing Engineering Laboratory
Managed Infrastructure
(NIST 820-01)***

Final Inspection Report No. OSE-19511/August 2009

Office of Audit and Evaluation



AUG - 7 2009

MEMORANDUM FOR: Dr. Patrick Gallagher
Deputy Director
National Institute of Standards and Technology

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

SUBJECT: National Institute of Standards and Technology
*FY 2009 FISMA Assessment of Manufacturing Engineering
Laboratory Managed Infrastructure (NIST 820-01)*
Final Inspection Report No. OSE-19511

This report presents the results of our Federal Information Security Management Act (FISMA) review of NIST's certification and accreditation of the Manufacturing Engineering Laboratory Managed Infrastructure.

We found that NIST's C&A process provided the authorizing official sufficient information to make a credible risk-based decision to approve system operation. However, the system security plan and control assessments, though generally adequate, need improvement, and our tests of selected security controls identified weaknesses that require remediation.

In its response to our draft report, NIST concurred with all our findings and fully concurred with all but one of our recommendations. NIST's response is summarized in the appropriate sections of the report where we also provide additional detail on the recommendation that NIST disagreed with and address some other minor points of disagreement. NIST's response is included in its entirety as appendix D.

We request that you provide us with 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. A plan of action and milestones should be used to communicate the plan as required by FISMA.

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

Attachment

cc: Suzanne Hilding, chief information officer, U.S. Department of Commerce
Simon Szykman, chief information officer, NIST
Howard Harary, acting director, Manufacturing Engineering Laboratory, NIST
Kenneth R. Glenn, chief, Information Technology Security and Networking
Division, NIST

Listing of Abbreviated Terms & Acronyms

| | |
|-------|---|
| AO | Authorizing Official |
| █ | █ |
| C&A | Certification and Accreditation |
| CIO | Chief Information Officer |
| DISA | Defense Information Systems Agency |
| █ | █ |
| █ | █ |
| █ | █ |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act of 2002 |
| IT | Information Technology |
| █ | █ |
| MEL | Manufacturing Engineering Laboratory |
| NIST | National Institute of Standards and Technology |
| OCIO | Office of the Chief Information Officer |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| █ | █ |
| SSP | System Security Plan |
| TCP | Transmission Control Protocol |
| URL | Uniform Resource Locator |
| █ | █ |

Synopsis of Findings

- System security plan was generally adequate but improvements are needed.
- Secure configuration settings were established for operating systems, but not for applications.
- Control assessments were generally adequate but certification weaknesses were found.
- OIG assessments found vulnerabilities requiring remediation.

Conclusion

- As a result of the Commerce Office of the Chief Information Officer (OCIO) review referred to as the “Smart Spot Check” and subsequent improvement of the system C&A package, the authorizing official received sufficient information to make a credible, risk-based decision to approve system operation. Furthermore, continuous monitoring is providing the authorizing official sufficient information about the operational status and effectiveness of security controls. NIST should address the minor deficiencies we identified as part of its continuous monitoring of system security.

Summary of NIST Response

In its response to our draft report, NIST concurred with our findings and fully concurred with all but one recommendation. NIST requested that recommendation 2.1 regarding secure configuration settings be changed to only address the development of secure configuration settings for [REDACTED] rather than all IT products in the system. NIST also proposed several modifications to tables 1 and 2 dealing with vulnerabilities identified by our control assessments.

In addition, NIST identified actions it has taken or plans to take to address our recommendations. NIST’s written response is included in its entirety as appendix D of this report.

OIG Comments

NIST generally concurred with our findings and all but one of our recommendations. We address specific elements of NIST’s response in the applicable sections of the report and have modified tables 1 and 2 based on NIST’s response.

Introduction

The Manufacturing Engineering Laboratory (MEL) Managed Infrastructure supports the lab's mission, which is to satisfy the measurements and standards needs of U.S. manufacturers in mechanical and dimensional metrology and advanced manufacturing technology by conducting research and development, providing services, and participating in standards activities.

The MEL Managed Infrastructure comprises managed workstations, servers, printers, and firewalls that provide file sharing, printing, authentication, fileserver access to scientific project data, and security services to the laboratory's staff and guest workers.

NIST has categorized the MEL Managed Infrastructure as a [REDACTED],

[REDACTED]

The system was certified and accredited in September 2007 and was reviewed in December 2007 by the Department's OCIO using the Smart Spot Check process. This process was created by the Department's OCIO to determine whether C&A packages developed by Commerce operating units conform to the Department's IT security policy and applicable NIST standards and guidelines. Improvements recommended by this review were incorporated into the C&A package we evaluated.

Findings and Recommendations

1. System Security Plan Was Generally Adequate but Improvements Are

- The system description correctly represented the system components and defined the accreditation boundary.
 - Component listing was accurate.
 - System boundaries and interconnections were clearly defined.
- Implementation descriptions for 2 of 23 NIST SP 800-53 security controls we targeted for review need improvement:
 - Unsuccessful Login Attempts (AC-7) does not define the time period during which invalid login attempts are enforced as required by NIST SP 800-53.
 - User Identification and Authentication (IA-2) is identified as a system-specific control but our assessment revealed that it has common control characteristics.
[REDACTED] servers are managed by MEL system administrators. Thus, this control should be identified as a hybrid control in the implementation description.
- [REDACTED] software is used by the system administrators for operational needs, but appropriate authorizations have not been obtained or documented in the SSP.
 - Department policy prohibits the use of [REDACTED] on Commerce IT systems unless it has been explicitly authorized in writing by an operating unit CIO in support of an official Commerce IT application. The policy also requires a copy of each such authorization to be sent to the Commerce CIO.
- The authorizing official and the senior agency information security officer had not approved the system security plan (SSP) prior to initiation of the security certification phase.
 - NIST certification and accreditation procedures have been revised to follow NIST 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, which requires approval of the SSP prior to security certification.

Recommendations

NIST should ensure that

- 1.1 the security control descriptions in the SSP are accurate and complete; and
- 1.2 waivers or special authorizations are obtained and documented in accordance with Department policy.

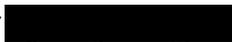
NIST Response

NIST concurred with this finding and our recommendations.

2. Secure Configuration Settings Were Established for Operating Systems, but Not for Applications

Background: The Department's IT security policy and NIST SP 800-53 require establishing and assessing secure configuration settings for IT products, which 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.

- Secure configuration settings and system-specific deviations were established and assessed for the following:

- However, NIST did not establish secure configuration settings for  and , two applications for which standardized configuration settings are available.

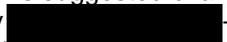
Recommendation

- 2.1 NIST should ensure that secure configuration settings are established, implemented, and assessed for all IT products in the system accreditation boundary in accordance with NIST SP 800-70, *Security Configuration Checklists Program for IT Products*.

NIST Response

NIST concurred with this finding but did not fully concur with this recommendation. NIST requested that it be changed to "NIST should ensure that secure configuration settings are established, implemented, and assessed for  for this system in accordance with NIST SP 800-70, Security Configuration Checklists Program for IT Products."

OIG Comments

NIST's suggested change indicates its willingness to establish secure configuration settings for only —IT products for which secure configuration guides or checklists are readily available. In addition to , MEL employs IT products such as , , which have configurable parameters that impact the security of the system; however, NIST has not established secure configuration settings for these products. Our recommendation that NIST establish secure configuration settings for all IT products is consistent with the NIST SP-800-53 control requirement (Configuration Settings (CM-6)) that organizations establish "mandatory configuration settings **for information technology products employed within the information system** [emphasis added]."

We recognize that configuration guides or checklists that can be tailored might not be readily available for some IT products employed within MEL. However, the current Department IT security policy, updated March 2009, indicates operating units "shall use [NIST] SP 800-70 to develop configuration setting checklists for IT products for which none are available."

We therefore reaffirm our recommendation.

3. Control Assessments Were Generally Adequate but Certification Weaknesses Were Found

The initial certification and accreditation package was completed in September 2007. After the system was accredited, the package underwent the Department's Smart Spot Check review process and the documentation was updated to address certification deficiencies that were identified. Continuous monitoring activities were also conducted in July 2008. We reviewed security control assessments from the updated package and evaluated continuous monitoring results.

- We reviewed certification assessments for a targeted set of 23 NIST SP 800-53 security controls and determined the following were not properly assessed on all IT products.
 - SSP control implementation descriptions state that spam controls are implemented on [REDACTED]. But Spam and Spyware (SI-8) assessment did not evaluate [REDACTED].
 - [REDACTED] (See finding 4.)
 - Authenticator Management (IA-5) requires that default authenticators (e.g., passwords) be changed. Assessment procedures called for determining whether default authenticators are present but the [REDACTED] were not evaluated.
 - We assessed the [REDACTED] for default authenticators and found they had been changed.
- To evaluate FY08 continuous monitoring we reviewed all control assessments and found that
 - controls required by NIST's continuous monitoring policy were assessed;
 - assessment procedures were developed and used to evaluate controls implemented on specific system components;
 - assessment results provided sufficient detail to support the outcome of assessment procedures; and
 - vulnerabilities identified during continuous monitoring were appropriately resolved, and the authorizing official was made aware of the results of the continuous monitoring effort.

Recommendations

NIST should ensure that assessments

3.1 address all aspects of the control as it is implemented in the system; and

3.2 are applied to all applicable IT products.

NIST Response

NIST concurred with this finding and our recommendations

4. OIG Assessments Found Vulnerabilities Requiring Remediation

As part of OIG's FY09 FISMA evaluation of the MEL Managed Infrastructure, we assessed a targeted set of system components to determine if selected security controls are properly implemented. We tailored our procedures to the infrastructure's specific control implementations.

Our assessments found the following vulnerabilities:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Recommendations

NIST should

- 4.1 ensure the vulnerabilities we identified are added to the system's plan of action and milestones and either remediated or accepted by the authorizing official; and
- 4.2 review the configuration settings that are not compliant with established checklists and correct them, document them as deviations, or incorporate them into the secure checklist.

NIST Response

NIST concurred with this finding and our recommendations but took exception to several entries in tables 1 and 2.

For the entry related to setting #18 in table 1, NIST noted that the deviation from the default setting for the component [REDACTED] is required to allow access to [REDACTED] and that the deviation for authentication servers has now been documented in its secure configuration [REDACTED].

For table 2, NIST indicated that the "[REDACTED]" service needs to be enabled for three of the components we identified. NIST also requested we remove the fully-qualified host name for the component "[REDACTED]"

OIG Comments

We added a note to table 1 to indicate that NIST reported documenting a deviation from setting #18 in its established checklist.

We deleted from table 2 the three components NIST identified as requiring the "[REDACTED]" service and removed the fully-qualified host name for "[REDACTED]" because it is not needed to address the "[REDACTED]" vulnerability we identified for that component.

Table 1. Secure Configuration Settings That Are Not Compliant With Established Checklists

| | | |
|------------|------------|------------|
| [REDACTED] | [REDACTED] | [REDACTED] |

Table 2. Vulnerabilities Identified Through OIG System Scanning Using Nessus

| Vulnerability | Port | Component | OIG Comments |
|---------------|------------|------------|--------------|
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |

Appendix A: Objectives, Scope, and Methodology

To meet the FY 2009 FISMA reporting requirements, we evaluated the NIST certification and accreditation for the Manufacturing Engineering Laboratory (MEL) Managed Infrastructure (NIST 820-01).

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 certification and accreditation, we reviewed all components of the package and interviewed NIST staff to clarify any apparent omissions or discrepancies in the documentation and gain further insight on the extent of the security assessment. We evaluated the system security plan descriptions and security assessment results for a targeted set of security controls and will give substantial weight to the evidence that supports the rigor of the security assessment when reporting our findings to OMB. (See appendix B for the controls we evaluated.)

In addition, we performed our own security control assessments on MEL Managed Infrastructure components. We chose a subset of the controls specified in NIST SP 800-53 for a moderate-impact system, and a subset of procedures from NIST SP 800-53A, which we tailored to NIST's 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. (See appendix C for the controls we assessed on MEL Managed Infrastructure components.)

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 NIST's certification test results. We assessed control implementations on five [REDACTED]

[REDACTED] components.

In addition, we examined the security plan descriptions, including related policy documents, and interviewed appropriate NIST personnel.

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 (Gold Disk) and NIST scripts
- Addition, modification, and deletion of operating system accounts
- Execution and analysis of Nessus vulnerability scans

Our assessment was limited in scope and should not be interpreted as the comprehensive review that a security certification for a [REDACTED] system would require. However, our assessments gave us direct assurance of the status of select aspects of important controls in MEL Managed Infrastructure and provided meaningful comparison to NIST's 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*, June 30, 2005
- 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*
 - 800-53, *Recommended Security Controls for Federal Information Systems*
 - 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
 - 800-70, *Security Configuration Checklists Program for IT Products*
 - 800-115, *Technical Guide to Information Security Testing and Assessment*

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

**Appendix B: Targeted Set of NIST SP 800-53 Security Controls
Evaluated During OIG Review of MEL Managed Infrastructure System
Security Plan and Security Assessment Results**

- Account Management (AC-2)
- Unsuccessful Login Attempts (AC-7)
- System Use Notification (AC-8)
- Session Lock (AC-11)
- Session Termination (AC-12)
- Wireless Access Restrictions (AC-18)
- Auditable Events (AU-2)
- Response to Audit Processing Failures (AU-5)
- Time Stamps (AU-8)
- Configuration Settings (CM-6)
- Least Functionality (CM-7)
- User Identification and Authentication (IA-2)
- Authenticator Management (IA-5)
- Water Damage Protection (PE-15)
- Rules of Behavior (PL-4)
- Vulnerability Scanning (RA-5)
- User Installed Software (SA-7)
- Boundary Protection (SC-7)
- Mobile Code (SC-18)
- Flaw Remediation (SI-2)
- Malicious Code Protection (SI-3)
- Information System Monitoring Tools and Techniques (SI-4)
- Spam Protection (SI-8)

Appendix C: NIST SP 800-53 Security Controls Assessed by OIG on MEL Managed Infrastructure Components

- Account Management (AC-2)
- Unsuccessful Login Attempts (AC-7)
- System Use Notification (AC-8)
- Session Lock (AC-11)
- Auditable Events (AU-2)
- Time Stamps (AU-8)
- Configuration Settings (CM-6)
- Least Functionality (CM-7)
- User Identification and Authentication (IA-2)
- Authenticator Management (IA-5)
- Rules of Behavior (PL-4)
- User Installed Software (SA-7)
- Mobile Code (SC-18)
- Flaw Remediation (SI-2)
- Malicious Code Protection (SI-3)



**UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology**

Gaithersburg, Maryland 20899-0001
OFFICE OF THE DIRECTOR

JUL 10 2009

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

From: Patrick Gallagher
Deputy Director

Subject: NIST Comments in Response to Draft Inspection Report No. OSE-19511 Entitled
*"FY 2009 FISMA Assessment of Manufacturing Engineering Laboratory
Managed Infrastructure"* (NIST 820-01), Draft Inspection Report No. OSE-19511

I would like to thank you for the opportunity to comment on your Draft Inspection Report No. OSE-19511, entitled *"FY 2009 FISMA Assessment of Manufacturing Engineering Laboratory Managed Infrastructure"* (NIST 820-01). In addition, I would like to compliment you on the thoroughness of your review.

NIST concurs with the majority of recommendations made in your draft report, and I assure you we will take all steps necessary to implement your recommendations. In the few cases where NIST does not fully concur with your recommendations, we have suggested that the language of the recommendation be changed, or we note that the recommendation is no longer appropriate due to changes in systems administration or configuration. NIST comments on the draft inspection report are found in the attachment to this letter.

Again, I would like to thank you for the opportunity to comment on this draft report, and assure you that NIST will implement your recommendations as soon as possible. If you have any questions concerning this response, please contact Stephen Willett on (301) 975-8707. Your efforts to improve NIST systems security are greatly appreciated.

Attachment

Response to FY 2009 FISMA Assessment of Manufacturing Engineering Laboratory Managed Infrastructure (NIST 820-01)

Draft Inspection Report No. OSE-19511/May 2009
Comments due June 12, 2009

1. System Security Plan Was Generally Adequate but Improvements Are Needed

Recommendations

NIST should ensure that

- 1.1 the security control descriptions in the SSP are accurate and complete; and
- 1.2 waivers or special authorizations are obtained and documented in accordance with Department policy.

NIST Response

NIST concurs with these findings and recommendations. See below for detailed responses.

| OIG Documented Deficiency | | NIST/MEL Remediation Plan/Justification | Testing Evidence and References |
|---|---|---|--------------------------------------|
| System Security Plan: Implementation description for two of twenty-three NIST SP 800-53 security controls we targeted for review need improvement | Unsuccessful Login Attempts (AC-7) does not define the time period during which invalid login attempts are enforced as required by NIST SP 800-53 | Corrected the MEL Procedures referenced in the SSP for this system. Corrected procedures included with the system documentation on the NIST OCIO secure share. | See System Security Plan for 820-01. |

| | | | |
|---|--|---|--|
| | <p>User Identification and Authentication (IA-2) is identified as a system-specific control but our assessment revealed that it has common control characteristics.</p> <p>[REDACTED]</p> <p>[REDACTED] servers are managed by MEL system administrators. Thus, this control should be identified as a hybrid control in the implementation description.</p> | <p>Corrected in the System Security Plan for 820-01 for the FY09 annual assessment.</p> | <p>See System Security Plan for 820-01.</p> |
| <p>[REDACTED] software is used by the system administrators for operational needs, but appropriate authorizations have not been obtained or documented in the SSP.</p> | <p>Department policy prohibits the use of [REDACTED] on Commerce IT systems unless it has been explicitly authorized in writing by an operating unit CIO in support of an official Commerce IT application. The policy also requires a copy of each such authorization to be sent to the Commerce CIO.</p> | <p>The NIST CIO's office is currently drafting appropriate authorizations for specific and necessary use of [REDACTED]</p> | <p>Appropriate authorizations will be obtained.</p> |
| <p>The authorizing official and the senior agency information security officer had not approved the system security plan (SSP) prior to initiation of the security certification phase.</p> | <p>NIST certification and accreditation procedures have been revised to follow NIST 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, which requires approval of the SSP prior to security certification.</p> | | |

2. Secure Configuration Settings Were Established for Operating Systems, but Not for Applications

Recommendation

2.3 NIST should ensure that secure configuration settings are established, implemented, and assessed for all IT products in the system accreditation boundary in accordance with NIST SP 800-70, Security Configuration Checklists Program for IT Products.

NIST Response

NIST concurs with this finding, but does not concur with the wording for this recommendation. Requested wording detailed red below.

in

| OIG Documented Deficiency | NIST/MEL Remediation Plan/Justification | Testing Evidence and References |
|---|---|--|
| <p>NIST did not establish secure configuration settings for [REDACTED] two applications for which standardized configuration settings are available</p> | <p>NIST currently uses established secure configuration settings for applications where standardized configuration settings are available such as [REDACTED] NIST is currently using established secure configuration settings from CIS and DISA.</p> | <p>See CIS and DISA websites for checklists. See recently accredited NIST systems for examples of use of such checklists at NIST. An example is SSP 181-04, where CIS checklists were used for both [REDACTED] The next testing cycle for 820-01 will use such checklists.</p> <p>NIST requests that the recommendation be changed to read: “NIST should ensure that secure configuration settings are established, implemented, and assessed for [REDACTED] for this system in accordance with NIST SP 800-70, Security Configuration Checklists Program for IT Products.”</p> |

3. Control Assessments Were Generally Adequate but Certification Weaknesses Were Found

Recommendations

NIST should ensure that assessments
 3.1 address all aspects of the control as it is implemented in the system; and
 3.2 are applied to all applicable IT products.

NIST Response

NIST concurs with these findings and these recommendations. See below for detailed responses.

| OIG Documented Deficiency | NIST/MEL Remediation Plan/Justification | Testing Evidence and References |
|--|---|---|
| <p>We reviewed certification assessments for a targeted set of twenty-three NIST SP 800-53 security controls and determined the following were not properly assessed on all IT products.</p> | <p>SSP control implementation descriptions state that spam controls are implemented on [REDACTED], but Spam and Spyware (SI-8) assessment did not evaluate [REDACTED]</p> | <p>The NIST CIO's office will ensure that [REDACTED] during the next testing cycle for 820-01.</p> |
| | <p>[REDACTED]</p> | <p>There is a current NIST CIO POA&M to address this issue NIST wide.</p> |
| | <p>Authenticator Management (IA-5) requires that default authenticators (e.g., passwords) be changed. Assessment procedures called for determining whether default authenticators are present but the [REDACTED] were not evaluated.</p> <ul style="list-style-type: none"> We assessed the [REDACTED] for default authenticators and found they had been changed. | <p>The NIST CIO's office will ensure that the [REDACTED] are properly evaluated for 820-01's next testing cycle.</p> |

4. OIG Assessments Found Vulnerabilities Requiring Remediation

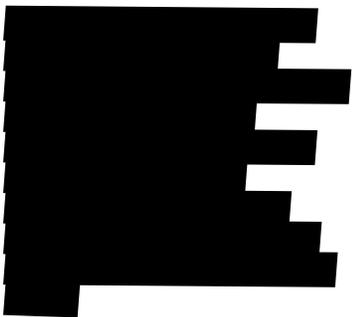
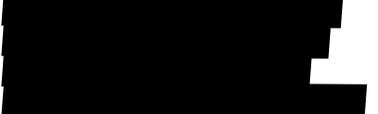
Recommendations

NIST should

- 4.1 ensure the vulnerabilities we identified are added to the system’s plan of action and milestones and either remediated or accepted by the authorizing official; and
- 4.2 review the configuration settings that are not compliant with established checklists and correct them, document them as deviations, or incorporate them into the secure checklist.

NIST Response

NIST concurs with these findings and these recommendations, with the exception of deviations documented in red below. Additionally NIST requests the removal of the fully qualified hostname from the final report (see note in Table 2 below). See below for detailed responses.

| OIG Documented Deficiency | NIST/MEL Remediation Plan/Justification | Testing Evidence and References |
|--|--|---------------------------------|
|  |  <p>The MEL IT Security Officer briefed the System Owner on the complete list of  and what was considered valid due to business justification.</p> | |

| | | | |
|---|-------------|--|--|
| [REDACTED] | [REDACTED] | There is a current NIST CIO POA&M to address this issue NIST wide. | |
| Noncompliant configuration settings. Secure configuration settings are not compliant with established checklists. | See Table 1 | See Table 1 below for specific responses. | |
| Other vulnerabilities. Our scanning using Nessus found several vulnerabilities, including [REDACTED] | See Table 2 | See Table 2 below for specific responses. | |

Table 1. Secure Configuration Settings That Are Not Compliant With Established Checklists

| <u>Operating System</u> | <u>Component Name</u> | <u>Noncompliant Settings</u> | <u>Remediation Plan</u> | <u>Justification or Testing Evidence</u> |
|-------------------------|-----------------------|------------------------------|-------------------------|--|
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |

| | | | | |
|------------|------------|------------|------------|------------|
| | | [REDACTED] | [REDACTED] | [REDACTED] |
| | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |

| | | | | |
|------------|------------|------------|------------|------------|
| | | [REDACTED] | [REDACTED] | [REDACTED] |
| | | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |

Table 2. Vulnerabilities Identified Through OIG System Scanning Using Nessus

| <u>Vulnerability</u> | <u>Port</u> | <u>Component</u> | <u>OIG Comments</u> | <u>NIST Remediation Plan</u> | <u>Justification</u> |
|----------------------|-------------|------------------|---------------------|------------------------------|----------------------|
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | |
| [REDACTED] | [REDACTED] | [REDACTED] | | [REDACTED] | |
| | [REDACTED] | [REDACTED] | | [REDACTED] | [REDACTED] |
| | [REDACTED] | [REDACTED] | | [REDACTED] | [REDACTED] |
| | [REDACTED] | [REDACTED] | | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | | [REDACTED] | [REDACTED] |

| | | | | | |
|------------|------------|------------|------------|------------|------------|
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| | | | | [REDACTED] | |