U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

National Institute of Standards and Technology

FY 2009 FISMA Assessment of Application Systems and Databases (NIST 183-06)

Final Inspection Report No. OSE-19512/August 2009

Office of Audit and Evaluation

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

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 Application Systems and Databases (NIST 183-06)
Final Inspection Report No. OSE-19512

This report presents the results of our Federal Information Security Management Act (FISMA) review of NIST's certification and accreditation of the Application Systems and Databases (ASD) system.

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. In the report, we note the need for minor improvements in security planning, secure configuration settings, and security control assessments. Our assessment of ASD security controls found vulnerabilities requiring remediation.

In its response to our draft report, NIST concurred with our findings and recommendations with several exceptions related to specific details. The response is summarized in the appropriate sections of the report where we also address the minor points of disagreement. NIST's response is included in its entirety as appendix C.

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
L. Dale Little, chief, Applications Systems Division, NIST
Kenneth R. Glenn, chief, Information Technology Security and Networking Division, NIST

Listing of Abbreviated Terms & Acronyms

ASD	Application Systems and Databases
C&A	Certification and Accreditation
CGI	Common Gateway Interface
COTS	Commercial off-the-shelf
CSAM	Cyber Security Assessment and Management
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
[redacted]	[redacted]
IT	Information Technology
ITSO	Information Technology Security Officer
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OS	Operating System
POA&M	Plan of Action & Milestones
SSO	System Security Officer
SSP	System Security Plan
SQL	Structured Query Language

Synopsis of Findings

- Revised system security plan was generally adequate, but security planning process needs improvement.
- Secure configuration settings were not established for all IT products.
- Control assessments produced reliable information for assessing risk, but some minor improvements are needed.
- OIG assessments found vulnerabilities requiring remediation.

Conclusion

- While there were deficiencies with security planning prior to the certification phase, NIST's certification and accreditation process, in particular its assessment of security controls, produced sufficient information for the authorizing official to make a credible, risk-based decision to approve system operation. 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 recommendations with several exceptions on select points in our report. It did not concur with the part of our finding that noted the security plan had been written by the certification team. NIST also did not concur with our security control assessment finding that there was insufficient disk space for [redacted] logs. And it did not concur with one of our examples of deficiencies with the NIST certification team's security control assessment.

One of NIST's remarks with respect to custom secure configuration checklists for [redacted] suggests its disagreement, in part, with our recommendation that NIST establish secure settings for **all** IT products in the system. And NIST's remarks on two items in our tables were non-responsive to the deficiencies we identified.

NIST also described actions it has taken or plans to take to address our recommendations.

NIST's written response is included in its entirety as appendix C of this report.

OIG Comments

NIST generally concurred with our findings and recommendations. We address several specific disagreements in the applicable sections of the report.

Introduction

The Application Systems and Databases system (ASD) consists solely of software. The system includes database containers, database management systems, and web application servers that support other NIST systems. ASD also includes applications that provide data object translation, data warehousing, and report generation capabilities. The hardware and associated operating systems hosting ASD software are not in the accreditation boundary and instead included in other NIST systems.

NIST has categorized ASD as a [redacted].

NIST initiated the certification and accreditation process in August 2007. Certification was completed in late December 2007 and, after an internal quality assurance and management review, the CIO authorized system operation on May 11, 2008.

Findings and Recommendations

1. Revised System Security Plan Was Generally Adequate, but Security Planning Process Needs Improvement

NIST first developed a single security plan for certifying and accrediting ASD. This initial plan covered the "parent" system only, consisting primarily of [redacted] products. NIST ultimately prepared three security plans for this system's accreditation—one for the parent system, and two subsystem plans for an application server and reporting tools.

- The initial system security plan did not fully address controls for the parent system and omitted subsystems altogether.
  - The initial security plan did not include major software components: [redacted]
  - No control enhancements required for the system were described.
  - Many control descriptions were deficient. (See table 1.)
    - Several controls were not accurately or completely described.
    - Several controls for an application [redacted] were not described.
    - Common and hybrid controls were not correctly identified.
  - Despite these deficiencies, the senior agency information security officer and the authorizing official formally accepted the initial security plan indicating the set of controls described "meets the security requirements for the system," and gave approval for the C&A "process to begin." NIST then began security certification activities.
  - A hardware server was removed from the accreditation boundary sometime during the security certification (system now consists of software only).
    - NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, calls for accreditation boundaries to be established before the certification phase begins.

- Along with assessing controls, NIST certification team members rewrote the parent security plan and created new subsystem security plans that served as the basis for the accreditation decision.
  - NIST told us that the system security officer and other administrators participated in the development of the final plans. However, the certification team's authorship of the security plans raises the possibility that security control requirements were solely based on security settings and implementations discovered during control assessments rather than a risk-based process to determine the necessary protections for information in ASD. In fact, many control descriptions in the revised security plan are direct quotes from the control assessment.
    - Scoping and tailoring control requirements should be driven by consideration of risk to the confidentiality, integrity, and availability of the information in the system. While certification teams should consult with system owners about the adequacy of the security plan, it is the system owner's role to maintain the plan based on input from various managers with system responsibilities.

- Revised system security plans generally addressed all required elements of the NIST SP 800-53 controls for each system component. However, some control descriptions need improvement. (See table 2.)

Recommendations

1.1 NIST authorizing officials and the senior agency information security officer should ensure that the scoping and tailoring of security controls and the security plan descriptions of system-specific implementations are completed before entering the certification phase so that control assessments have appropriate standards against which controls can be measured.

1.2 NIST should rectify the deficiencies identified in table 2.

NIST Response

NIST concurred with this finding and our recommendations. NIST indicated it would ensure future initial security plans include sufficient detail. However, it took exception to the part of our finding that discusses the certification team's involvement in writing the revised security plans. NIST suggested that the certification team's involvement was less than we depicted—NIST said a member only provided assistance by rewriting some parts—and that security requirements were "defined, reviewed, and approved" by NIST managers prior to the accreditation decision.

NIST indicated it had remediated or planned to remediate the deficiencies in the revised security plans we identified in table 2.

OIG Comments

NIST's depiction of the certification team's involvement is different from what we learned during the course of our evaluation. The ASD system security officer told us that he had prepared an initial draft of the parent system plan and then "turned it over" to the certification team. The team member who rewrote much of the parent plan and wrote the subsystem plans also did much of the testing for the security certification. When we met him, he told us he wrote the plans after the security certification. And, as we note in the finding, many of the descriptions of controls in the revised plans were direct quotes from the security control assessment.

We acknowledge what NIST told us during the evaluation—that the writing of the plans was an iterative process between the certification team and the system security officer and both worked toward agreed-upon descriptions of controls. This aspect of our finding was merely to caution NIST that its approach deviated from the process described in NIST SP 800-37 and, as discussed in our finding, could result in a less-than-adequate determination of security requirements.

2. Secure Configuration Settings Were Not Established for All IT Products

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 were established for the [redacted] but not for other significant applications in the system.
  - [redacted] have standardized secure configuration checklists available. (Checklists provide predefined secure configuration settings that can be used to establish system-specific settings.)
  - NIST explained that a program-level POA&M exists to address the need to develop secure configuration checklists for applications. However, this POA&M (#26334 in CSAM) was closed June 30, 2008, without developing any additional secure configuration checklists applicable to ASD applications.
  - To illustrate the importance of utilizing secure configuration checklists, we assessed configuration settings for two of the system's [redacted]) against the Defense Information Systems Agency's (DISA) [redacted] security checklist.
    - We selected 24 technical settings with significant impact (DISA's category 1 or 2[1]) from the checklist.
      - [redacted] results included 10 category 2 vulnerabilities.
      - [redacted] results included 8 category 2 vulnerabilities. (See table 3.)
    - These vulnerabilities might have been resolved if a secure configuration checklist were implemented for this application. (It is also possible that remediation of some vulnerabilities may prevent the successful operation of the legacy applications, but that risk should be identified and appropriately considered according to the methodology in NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*.)

- The NIST [redacted] secure configuration checklist[2] was not tailored for the ASD system.
  - NIST has a secure configuration checklist for [redacted] that serves as an enterprise-wide standard. However, NIST told us that prior to assessment, the checklist had not been tailored to the system-specific requirements of ASD.
  - NIST's certification team, along with system administrators, determined the appropriate settings for the sample of databases assessed. However, configuration settings for other databases in the system need to be established

[1] DISA checklists use severity codes to denote the significance of vulnerabilities resulting from improperly applied configuration settings. Category 1 vulnerabilities allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall. Category 2 vulnerabilities help an attacker access a machine, compromise sensitive data, or bypass a firewall.

[2] NIST SP 800-70, *Security Configuration Checklists Program for IT Products*, requires system owners to develop secure configuration checklists (a list of secure configuration settings) for IT products. NIST OCIO uses the term "guides" as the equivalent of checklists.

and documented. This activity, part of tailoring security control requirements, is the responsibility of the system owner.

- The description, assessment, and remediation of configuration settings were inappropriately assigned to security control Baseline Configuration (CM-2).
  - CM-2 requires the creation of a baseline configuration that describes the makeup of each component and its logical placement within the information system.
  - Configuration Settings (CM-6) is the appropriate control. It requires the establishment, configuration, documentation, and enforcement of configuration settings to the most restrictive mode consistent with operational requirements.

- Assessments of [redacted] configuration settings were adequate.
  - Assessment results were supported by adequate evidence that was appropriately referenced in summary assessment results.
  - Settings were evaluated from an appropriate sample of databases.

- [redacted] configuration vulnerabilities were not adequately remediated.
  - During the certification process, NIST added an action item to its POA&M (CSAM #26134) to address vulnerabilities identified during the assessment of secure configuration settings. The item directs that "staff apply the NIST [redacted] Secure Configuration Guidelines consistently among all databases by 9/30/2008." This POA&M item was marked completed on September 2, 2008.
    - NIST OCIO indicated it completed the POA&M based on staff response to a status request and that validation testing will be performed at a later date, as part of continuous monitoring activities. However, Appendix E of the Department's IT Security Program Policy and Minimum Implementation Standards requires the ITSO to have tested the POA&M item's implementation before categorizing the item as complete.
  - We found that while NIST has remediated many of the vulnerabilities identified in its assessment, the configuration settings were not applied consistently among the databases we assessed.
    - We assessed 86 of NIST's defined configuration settings for [redacted]. NIST had identified 33 improperly applied settings in its own assessment. Of these 33, we found that 22 were properly applied in the databases we assessed. The remaining 11 improper settings NIST identified were present on one or more databases included in our assessment. (See table 4.)
    - We also found 3 configuration settings (listed below) that NIST had marked as "Satisfied" because "the database administrator changed the setting" to the correct value, implying that the change had been made at the time of the assessment. These settings were either not successfully corrected as stated or the incorrect settings were reintroduced following the change.
      - [redacted]
      - [redacted]
      - [redacted]
    - We also found 6 improper settings NIST did not identify in its security certification. (See table 5.)

Recommendations

NIST should

2.1 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*;

2.2 tailor the NIST [redacted] secure configuration checklist to the specific operational requirements of ASD;

2.3 only close POA&M items after validation testing or examination demonstrates that the planned remedial action(s) succeeded; and

2.4 create a new POA&M item to track the remediation of [redacted] vulnerabilities in databases.

NIST Response

NIST indicated it concurred with this finding and our recommendations except for an item listed in table 5 regarding disk space available for [redacted] on a particular server. We identified the remaining available space to be insufficient at 5 MB; NIST noted that the remaining space was actually 5 GB, which was adequate.

In response to check # 73 of table 5, which deals with the [redacted]

NIST indicated that it would tailor an [redacted] secure configuration checklist for ASD and that it identifies secure configuration guides for applications when they exist and customizes them for each situation, depending on functional requirements.

OIG Comments

NIST rightly pointed out our error in interpreting available disk space for the database in question and we have removed the item from table 5.

With respect to check #73, NIST's remarks were unresponsive to that particular issue. The [redacted]

NIST's explanation for how it defines secure configuration settings for applications suggests that it will do so only if a secure configuration guide or checklist is available ("when they exist"). However, Department policy mandates that operating units develop their own secure settings for IT products if necessary. The current Department IT security policy, updated March 2009, states that operating units "shall use [NIST] SP 800-70 to develop configuration setting checklists for IT products for which none are available." Therefore, we reaffirm recommendation 2.1.

3. Control Assessments Produced Reliable Information for Assessing Risk, but Some Minor Improvements Are Needed

- System-specific control assessments were generally adequate.
  - Assessments were performed on an adequate set of system components.
  - Results, in general, were sufficiently supported by evidence.
  - Procedures were adequate to assess security control requirements.

- However, three control assessments were not sufficient to assess security control implementations. (See table 6.)

- Assessment results and analysis for some controls provided by other systems were not included in certification assessments. As a result, potential risk associated with these controls was not properly identified. (See table 7.)
  - The ASD system inherits remaining vulnerabilities related to controls provided by other systems.

Recommendations

NIST should

3.1 reassess the controls listed in table 6 as part of continuous monitoring; and

3.2 present assessment results for controls provided by other systems, as identified in table 7, to the authorizing official.

NIST Response

NIST indicated it concurred with this finding and our recommendations. However, NIST did not agree with one of the security control assessment deficiencies we identified in table 6. NIST indicated its secure configuration script did check settings related to [redacted]. It acknowledged the documented assessment result "was lacking sufficient detail" and should have referenced the secure configuration script. And NIST offered explanations as to why the script identified inconsistent settings in its databases: [redacted]

With respect to the [redacted] **control assessment** deficiency, NIST indicated that it "updated the Parent SSP, [redacted] SSP and [redacted] SSP, control [redacted] to remediate this deficiency."

OIG Comments

Security control assessment involves not just obtaining the necessary data (e.g., through scripts) but analyzing the data to determine the actual risk involved. In this case, the certification team, based on an interview and examination of requirements, concluded that this control [redacted] was being effectively implemented in the system. At the same time, the script data showed that the control was not consistently implemented in ASD databases. Therefore, the assessment result was not accurate and does represent a deficiency in NIST's assessment process. NIST appears to partly recognize the deficiency based on its response indicating it "will be more explicit when describing how controls are tested."

NIST was non-responsive to the [redacted] control assessment deficiency identified in table 6. Updating the security plan is not a corrective action for a deficient control assessment. As the table indicates, “This control should be assessed where it is implemented. An examination of the [redacted] for a representative set of system components is necessary to determine if information system [redacted].”

4. OIG Assessments Found Vulnerabilities Requiring Remediation

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

- OIG assessments identified several vulnerabilities that need to be addressed. (See table 8 for details.) These vulnerabilities include the following:

[redacted]

Recommendation

4.1 NIST should ensure the vulnerabilities identified in table 8 are added to the system's POA&M and remediated during continuous monitoring.

NIST Response

NIST concurred with this finding and recommendation.

Table 1. Deficiencies in Initial Security Plan

Deficiency	Controls
Controls not accurately or completely described	[redacted]
Controls for [redacted] application not described	[redacted]
Common and hybrid controls not correctly identified	[redacted]

Table 2. Deficiencies in Revised Security Plan

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted].

Table 2. Deficiencies in Revised Security Plan

Control	Security Plan Description (excerpts)	OIG Comments
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 2. Deficiencies in Revised Security Plan

Control	Security Plan Description (excerpts)	OIG Comments
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 2. Deficiencies in Revised Security Plan

Control	Security Plan Description (excerpts)	OIG Comments
[redacted]	[redacted]	[redacted]

Table 3 [redacted] Vulnerabilities

DISA Vulnerability Key	DISA Required Setting	OIG Assessment Results	OIG Comments
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 3. [redacted] Vulnerabilities

DISA Vulnerability Key	DISA Required Setting	OIG Assessment Results	OIG Comments
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 3. [redacted] Vulnerabilities

DISA Vulnerability Key	DISA Required Setting	OIG Assessment Results	OIG Comments
[redacted]	[redacted]	[redacted]	[redacted]

Table 4: Persistent Improper Settings in [redacted]

Checklist Check #	NIST Requirement (Full Quotation)	OIG Assessment Results
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 4: Persistent Improper Settings in [redacted]

Checklist Check #	NIST Requirement (Full Quotation)	OIG Assessment Results
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 5. Additional Improper Settings in [redacted]

Checklist Check #	NIST Requirement (Full Quotation)	OIG Assessment Results
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 5. Additional Improper Settings in [redacted]

Checklist Check #	NIST Requirement (Full Quotation)	OIG Assessment Results
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 6. NIST Security Control Assessment Deficiencies

Control	NIST Assessment Procedure (Full Quotation)	NIST Assessment Results (Full Quotation)	OIG Comments
[redacted]	[redacted]	[redacted]	[redacted]

Table 6. NIST Security Control Assessment Deficiencies

Control	NIST Assessment Procedure (Full Quotation)	NIST Assessment Results (Full Quotation)	OIG Comments
[redacted]	[redacted]	[redacted]	[redacted]

Table 6. NIST Security Control Assessment Deficiencies

Control	NIST Assessment Procedure (Full Quotation)	NIST Assessment Results (Full Quotation)	OIG Comments
[redacted]	[redacted]	[redacted]	[redacted]

Table 7. Controls Lacking Results and Supporting Evidence of Assessments for Other Systems

Control Number	ASD Applications Inheriting Controls	NIST System(s) Implementing the Control
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 8. Vulnerabilities Identified by OIG Assessment of Selected Security Controls

Control	Vulnerability	System Component	OIG Assessment Details
[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 8. Vulnerabilities Identified by OIG Assessment of Selected Security Controls

Control	Vulnerability	System Component	OIG Assessment Details
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	[redacted]
		[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 8. Vulnerabilities Identified by OIG Assessment of Selected Security Controls

Control	Vulnerability	System Component	OIG Assessment Details
[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 Application Systems and Databases system (NIST 183-06).

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 C&A 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 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.) To evaluate the system security plans, we reviewed all required security controls to determine whether and to what extent the certification team's role in developing the plans had any significant negative effects. In our initial review, we found that assessment results for some controls implemented by other systems had not been properly documented. In this regard we expanded our scope by looking at all required controls to identify those that were provided by other systems and whether they had been assessed and included in the C&A package.

In addition, we performed our own assessments of the same control set we used to evaluate NIST's control assessments (appendix B), with the exception of control PL-5 Privacy Impact Assessment. We conducted our assessment using a subset of procedures from NIST SP 800-53A, which we tailored to ASD's specific control implementations. We did not attempt to perform a complete assessment of each control; instead we chose to focus on specific technical and operational elements.

We assessed controls on key classes of IT components (in this system, 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 the seven [redacted], and controls for the [redacted]. 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 NIST-developed scripts and DISA checklists
- Addition, modification, and deletion of accounts

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 system controls 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: NIST SP 800-53 Security Controls Evaluated During OIG Review of ASD

- Account Management (AC-2)
- Separation of Duties (AC-5)
- Unsuccessful Login Attempts (AC-7)
- Auditable Events (AU-2)
- Audit Storage Capacity (AU-4)
- Response to Audit Processing Failures (AU-5)
- Audit Monitoring, Analysis and Reporting (AU-6)
- Time Stamps (AU-8)
- Protection of Audit Information (AU-9)
- Configuration Settings (CM-6)
- Information System Backup (CP-9)
- User Identification and Authentication (IA-2)
- Authenticator Management (IA-5)
- Privacy Impact Assessment (PL-5)
- Vulnerability Scanning (RA-5)
- Flaw Remediation (SI-2)

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-19512 Entitled *"FY 2009 FISMA Assessment Application Systems and Databases" (NIST 183-06)*, Draft Inspection Report No. OSE-19512

I would like to thank you for the opportunity to comment on your Draft Inspection Report No. OSE-19512, entitled *"FY 2009 FISMA Assessment Application Systems and Databases" (NIST 183-06)*. 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 a 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

NIST

1. Revised System Security Plan Was Generally Adequate, but Security Planning Process Needs Improvement

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 these recommendations, with the exception of deviations documented in red in this section (Page 2). See below for detailed responses.

OIG Documented Deficiency		Remediation Plan / Justification
The initial system security plan did not fully address controls for the parent system and omitted subsystems altogether.	The initial security plan did not include major software components: [redacted]	**NIST will ensure that future initial SSPs will provide sufficient detail before continuing with the C&A process. These deficiencies were fixed in the final SSP submission.**
	No control enhancements required for the system were described.	
	Several controls were not accurately or completely described. See Table 1.	
	Several controls for an application [redacted] were not described.	
	Common and hybrid controls were not correctly identified.	
	A hardware server was removed from the accreditation boundary sometime during the security certification (system now consists of software only). NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, calls for accreditation boundaries to be established before the certification phase begins.	

Along with assessing controls, NIST certification team members rewrote the parent security plan and created new subsystem security plans that served as the basis for the accreditation decision.	NIST told us that the system security officer and other administrators participated in the development of the final plans. However, the certification team's authorship of the security plans raises the possibility that security control requirements were solely based on security settings and implementations discovered during control assessments rather than a risk-based process to determine the necessary protections for information in ASD. In fact, many control descriptions in the revised security plan are direct quotes from the control assessment. Scoping and tailoring control requirements should be driven by consideration of risk to the confidentiality, integrity, and availability of the information in the system. While certification teams should consult with system owners about the adequacy of the security plan, it is the system owner's role to maintain the plan based on input from various managers with system responsibilities.	**NIST does not concur with this finding. While the NIST certification team member provided assistance by rewriting some parts of the security documentation, the requirements, were defined, reviewed and approved by the SSO and System Owner (SO), prior to the presentation of the package to the Authorizing Official (AO) for the final accreditation decision.**
Revised system security plans generally addressed all required elements of the NIST SP 800-53 controls for each system component. However, some control descriptions need improvement. (See table 2.)		**See Table 2, Pages 10 through 13.**

2. Secure Configuration Settings Were Not Established for All IT Products

Recommendations

NIST should ensure that

2.1 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*;
2.2 tailor the NIST [redacted] secure configuration checklist to the specific operational requirements of ASD;
2.3 only close POA&M items after validation testing or examination demonstrates that the planned remedial action(s) succeeded; and
2.4 create a new POA&M item to track the remediation of [redacted] vulnerabilities in the databases

NIST Response

NIST concurs with these findings and these recommendations, with the exception of deviations documented in red in Table 5, Page 20. See below for detailed responses.

OIG Documented Deficiency		Remediation Plan / Justification
Secure configuration settings were established for the [redacted] but not for other significant applications in the system.	[redacted] have standardized secure configuration checklists available. (Checklists provide predefined secure configuration settings that can be used to establish system specific settings.)	**See Tables 3 through 5, Pages 14 through 21.**
	NIST explained that a program-level POA&M exists to address the need to develop secure configuration checklists for applications. However, this POA&M (#26334 in CSAM) was closed June 30, 2008, without developing any additional secure configuration checklists applicable to ASD applications.	**NIST will ensure that future program-level POA&Ms that have such a broad scope are fully reviewed for completeness before being marked as complete.**
	To illustrate the importance of utilizing secure configuration checklists, we assessed configuration settings for two of the system's [redacted] against the Defense Information Systems Agency's (DISA) [redacted] security checklist. We selected 24 technical settings with significant impact (DISA's category 1 or 2[1]) from the checklist. • [redacted] results included 10 category 2 vulnerabilities. • [redacted] results included 8 category 2 vulnerabilities. (See table 3).	**See Table 3, Pages 14 through 16.**

	These vulnerabilities might have been resolved if a secure configuration checklist were implemented for this application. (It is also possible that remediation of some vulnerabilities may prevent the successful operation of the legacy applications, but that risk should be identified and appropriately considered according to the methodology in NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*.)	**See Tables 3 through 5, Pages 14 through 21.**
The NIST [redacted] secure configuration checklist[2] was not tailored for the ASD system.	NIST has a secure configuration checklist for [redacted] that serves as an enterprisewide standard. However, NIST told us that prior to assessment, the checklist had not been tailored to the system-specific requirements of ASD. NIST's certification team, along with system administrators, determined the appropriate settings for the sample of databases assessed. However, configuration settings for other databases in the system need to be established and documented. This activity, part of tailoring security control requirements, is the responsibility of the system owner.	**A POA&M (CSAM POA&M 34348) has been created to document and implement a tailored secure configuration guide for [redacted]. NIST identifies secure configuration guides for applications when they exist and customize them for each situation, depending on functional requirements.**
The description, assessment, and remediation of configuration settings were inappropriately assigned to security control Baseline Configuration (CM-2).	CM-2 requires the creation of a baseline configuration that describes the makeup of each component and its logical placement within the information system. Configuration Settings (CM-6) is the appropriate control. It requires the establishment, configuration, documentation, and enforcement of configuration settings to the most restrictive mode consistent with operational requirements.	**See Table 2, CM-2 row, Page 11.**
[redacted] configuration vulnerabilities were not adequately remediated.	During the certification process, NIST added an action item to its POA&M (CSAM #26134) to address vulnerabilities identified during the assessment of secure configuration settings. The item directs that "staff apply the NIST [redacted] Secure Configuration Guidelines consistently among all databases by 9/30/2008." This POA&M item was marked completed on September 2, 2008. NIST OCIO indicated it completed the POA&M based on staff response to a status request and that validation testing will be performed at a later date, as part of continuous monitoring activities. However, Appendix E of the Department's IT Security Program Policy and Minimum Implementation Standards requires the ITSO to have tested the POA&M item's implementation before categorizing the item as complete.	**In the future, sufficient evidence will be collected before marking a POA&M as complete.**

	We assessed 86 of NIST's defined configuration settings for [redacted] NIST had identified 33 improperly applied settings in its own assessment. Of these 33, we found that 22 were properly applied in the databases we assessed. The remaining 11 improper settings NIST identified were present on one or more databases included in our assessment. (See table4.)	**See Table 4, Pages 17 through 19.**
	We also found 3 configuration settings (listed below) that NIST had marked as "Satisfied" because "the database administrator changed the setting" to the correct value, implying that the change had been made at the time of the assessment. These settings were either not successfully corrected as stated or the incorrect settings were reintroduced following the change. • [redacted] • [redacted] • [redacted]	**Two issues were identified that resulted in inconsistent configuration settings.** **1.** [redacted] [redacted]
	We also found 6 improper settings NIST did not identify in its security certification. (See table 5.)	**See Table 5, Pages 20 through 21.**

3. Control Assessments Produced Reliable Information for Assessing Risk, but Some Minor Improvements Are Needed

Recommendations

NIST should ensure that assessments

3.1 reassess the controls listed in table 6 as part of continuous monitoring; and
3.2 present assessment results for controls provided by other systems, as identified in table 7, to the authorizing official.

NIST Response

NIST concurs with these findings and these recommendations, with the exception of deviations documented in red in Table 6, Page 22. See below for detailed responses.

OIG Documented Deficiency		Remediation Plan / Justification
Three control assessments were not sufficient to assess security control implementations. (See table 6.)		**See Table 6, Pages 22 through 25.**
Assessment results and analysis for some controls provided by other systems were not included in certification assessments. As a result, potential risk associated with these controls was not properly identified. (See table 7.).	The ASD system inherits remaining vulnerabilities related to controls provided by other systems.	**See Table 7, Page 26.**

4. OIG Assessments Found Vulnerabilities Requiring Remediation

Recommendations

NIST should

4.1 NIST should ensure the vulnerabilities identified in table 8 are added to the system's POA&M and remediated during continuous monitoring.

NIST Response

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

OIG Documented Deficiency		Remediation Plan / Justification
OIG assessments identified several vulnerabilities that need to be addressed. (See table 8 for details.) These vulnerabilities include the following:	[redacted]	**See Table 8, Pages 27 through 29.**

Appendix: **Tables**

Table 1. Deficiencies in Initial Security Plan		
Deficiency	Controls	Remediation Plan/Justification
Controls not accurately or completely described	[redacted]	**NIST will ensure that future initial SSPs will provide sufficient detail before continuing with the Certification and Accreditation (C&A) process. These deficiencies were fixed in the final SSP submission.**
Controls for [redacted] application not described	[redacted]	
Common and hybrid controls not correctly identified	[redacted]	

Table 2. Deficiencies in Revised Security Plan

Control	Security Plan Description (excerpts)	OIG Comments	Remediation Plan/ Justification
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]

Table 3 [redacted] Vulnerabilities

DISA Vuln Key	DISA Required Setting	OIG Assessment Results	OIG Comments	Remediation Plan / Justification
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	

[redacted]

[redacted]

Table 4: Persistent Improper Settings in [redacted]

Checklist Check #	NIST Requirement (Full Quotation)	OIG Assessment Results	Remediation Plan / Justification
[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]	

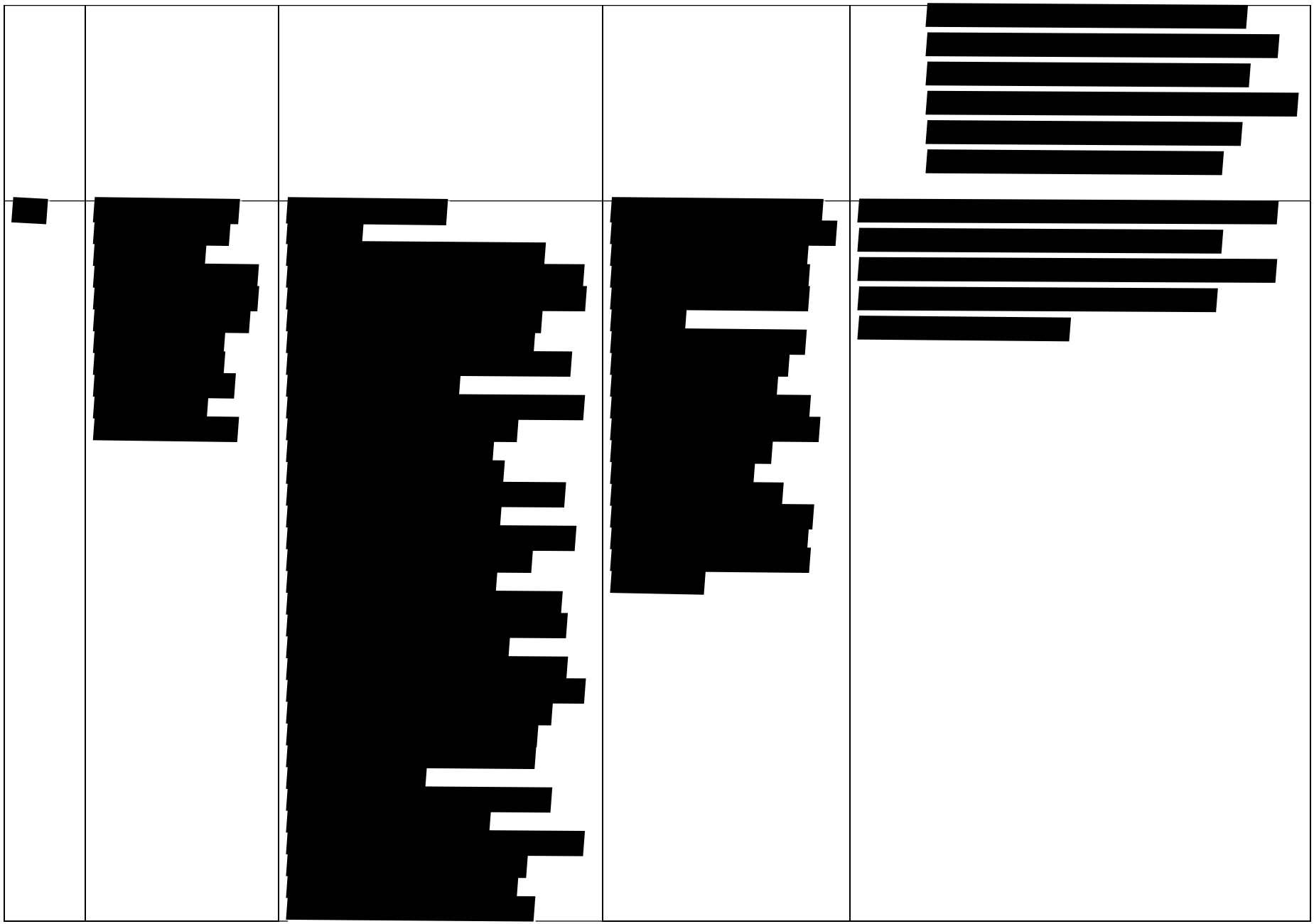
Table 5. Additional Improper Settings in [redacted]

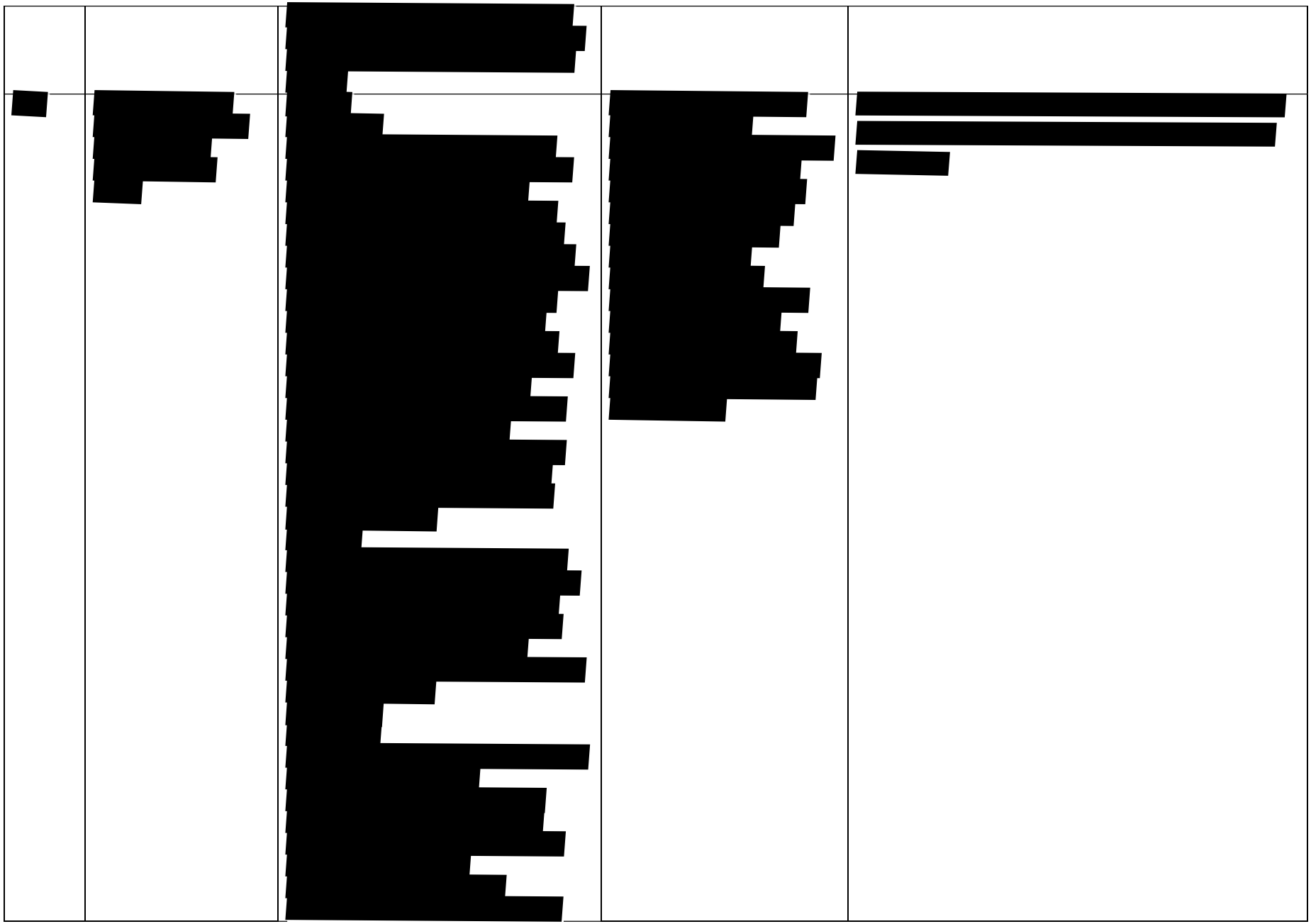
Checklist Check #	NIST Requirement (Full Quotation)	OIG Assessment Results	Remediation Plan / Justification
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

Table 6. NIST Security Control Assessment Deficiencies

Control	NIST Assessment Procedure (Full Quotation)	NIST Assessment Results (Full Quotation)	OIG Comments	Remediation Plan / Justification
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]





		[redacted]		

Table 7. Controls Lacking Results and Supporting Evidence of Assessments for Other Systems			
Control Number	ASD Applications Inheriting Controls	NIST System(s) Implementing the Control	Remediation Plan / Justification
[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 8. Vulnerabilities Identified by OIG Assessment of Selected Security Controls

Control	Vulnerability	System Component	OIG Assessment Details	Remediation Plan/ Justification
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]