OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

EPA's Computer Security Self-Assessment Process Needs Improvement

Report No. 2003-P-00017

September 30, 2003

Report Contributors:

Ed Densmore
Debbie Hunter
Martin Bardak
Teresa Richardson
Michael Young
Bill Coker

Abbreviations

ASSERT	Automated Security Self-Evaluation and Reporting Tool
EPA	Environmental Protection Agency
FISMA	Federal Information Security Management Act
GISRA	Government Information Security Reform Act
IT	Information Technology
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OIG	Office of Inspector General
OMB	Office of Management and Budget

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

SEP 30 2003

MEMORANDUM

SUBJECT: EPA's Computer Security Self-Assessment Process Needs Improvement
Audit Report No. 2003-P-00017

FROM: for Patricia H. Hill
Director, Business Systems (2421T)

TO: Mark Day
Director, Office of Technology, Operations, and Planning (2831T)

This is our final report regarding the Environmental Protection Agency's (EPA's) computer security self-assessment process. This audit report contains findings that describe problems the Office of Inspector General (OIG) has identified and corrective actions the OIG recommends. This audit report represents the opinion of the OIG, and the findings contained in this audit report do not necessarily represent the final EPA position. Final determinations on matters in this audit report will be made by EPA managers in accordance with established EPA audit resolution procedures.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response within 90 calendar days of the date of this report. You should include a corrective action plan for agreed upon actions, including milestone dates. We have no objection to the further release of this report to the public. For your convenience, this report will be available at http://www.epa.gov/oigearth/eroom.htm.

If you or your staff have any questions, please contact me at (202) 566-0894, or the Assignment Manager, Ed Densmore, at (202) 566-2565.

cc: Director, Technical Information Security Staff

Executive Summary

Management has taken positive actions to establish a computer security self-assessment process. However, additional areas need to be addressed to provide greater assurance that the Environmental Protection Agency's (EPA's) information technology security is accurately measured.

EPA's Office of Environmental Information (OEI) uses self-assessments to collect security-related information about its systems and report the consolidated results to the Office of Management and Budget. OEI took several significant actions to help program and regional personnel complete and report on self-assessments. OEI converted the self-assessment questionnaire into an Automated Security Self-Evaluation and Reporting Tool (ASSERT), a web-based format to facilitate compiling and reporting results, and provided step-by-step instructions on its use. Further, OEI reconciled EPA's system inventory to budget documentation.

Despite these positive efforts, improvements are needed in order for the Agency to place reliance on its computer self-assessment process. Specifically:

- Thirty-six percent of the critical self-assessment responses in our review were inaccurate or unsupported. Approximately 9 percent were inaccurate and 27 percent unsupported. As a consequence, the responses to the self-assessment questions we reviewed did not identify or support the current security status of those systems.

- EPA's system inventory did not identify all major applications. As a result, not all major applications completed a self-assessment or were included in the self-assessment for the applicable general support system.

- EPA management did not provide proper oversight to ensure implementation of authentication/identification security controls, which increased the potential for unauthorized access, misuse, and system downtime.

- EPA did not adequately plan for systems controls. As a result, management authorized systems to operate without being provided adequate information on the impact these risks had on operations.

These weaknesses were caused primarily because OEI does not have a systematic program to ensure that system controls are accurately presented and implemented throughout the Agency. To improve the self-assessment process, OEI's Director for Technology, Operations, and Planning needs to implement a systematic monitoring and evaluation program. Only then can management place reliance on the collected data and make informed judgments and investments.

In a memorandum dated July 15, 2003, OEI's Director for Technical Information Security responded to our draft report (Appendix B) and concurred with most of our recommendations. However, OEI raised concerns regarding the breadth of some finding statements, and did not agree that the audit's sampling and evaluation methodology supported a broad, Agency-wide conclusion regarding all technical controls. As such, we modified the report to clarify that the findings pertained to the critical self-assessment questions and responses we reviewed. Furthermore, although the sample was judgmental, we believe the national systems selected provided adequate coverage of EPA's program offices, as well as different types of Agency data (e.g., financial, enforcement/compliance, and systems containing environmental data). However, we modified the report language from "technical controls" to "authentication/identification controls" in order to more specifically reflect the work that was performed.

Table of Contents

Chapter 1
Introduction

Purpose

The objective of this audit was to review the Agency's policies, procedures, and practices regarding EPA's self-assessment of major applications and general support systems. Specifically, we determined whether:

- Computer security self-assessments were accurate and complete.
- EPA identified all major applications.
- Major application systems used authentication and identification controls to protect against unauthorized access or misuse.
- Systems security plans were documented, approved, and reviewed, and were consistent with National Institute of Standards and Technology (NIST) guidance.

We initially planned to identify both general support systems and major applications. Due to a software limitation involving EPA's network, we could not verify that all general support systems were listed on the systems inventory.

Background

The Federal Information Security Management Act (FISMA) and its predecessor, the Government Information Security Reform Act (GISRA), require all Federal agencies to conduct annual reviews of their security program and to report the results of those assessments to the Office of Management and Budget (OMB). OMB reviews the assessment results to determine how well agencies implemented security requirements. Starting in fiscal 2002, OMB directed agencies to use the *Federal Information Technology (IT) Security Assessment Framework* developed by the Federal Chief Information Officers Council, as well as the self-assessment methodology developed by and outlined in NIST Special Publication 800-26, to conduct these reviews.

Self-assessments provide a method for agency officials to determine the current status of the overall information security program and, where necessary, establish targets for improvement. The self-assessment methodology developed by NIST includes a questionnaire to help agencies assess how well information security controls have been implemented on every general support system and major

application. The NIST self-assessment questionnaire utilizes an extensive list of specific control objectives and techniques against which the security of a system can be measured. The questionnaire is comprised of over 200 questions that address 34 critical elements of security. To measure the progress of effectively implementing the needed security control, five levels of effectiveness are used to assess each security control question, as shown in Table 1:

Table 1: Five Levels of Security Effectiveness

Level	Name	Description
1	Policy	Control objective is documented in a security policy
2	Procedures	Security controls are documented as procedures
3	Implemented	Procedures have been implemented
4	Tested	Procedures and security controls are tested and reviewed
5	Integrated	Procedures and security controls are fully integrated into a comprehensive program

These five levels provide a standardized approach to assessing the status of security controls for major applications and general support systems. Per NIST guidance, the method for answering the questions can be based primarily on an examination of relevant documentation and a rigorous examination and test of the controls.

During fiscal 2002, EPA's Office of Environmental Information (OEI) developed EPA's Automated Security Self-Evaluation and Reporting Tool (ASSERT), a web-based version of NIST 800-26 *Security Self-Assessment Guide for Information Technology Systems* questionnaire. OEI subsequently tasked system owners to complete a self-assessment for every major application and general support system.

Scope and Methodology

We conducted audit field work from January 2003 to April 2003 at EPA Headquarters and Regions 1, 2, 3, 5, and 6. To accomplish this audit's objectives, we used a variety of Federal and Agency criteria, including OMB Circular A-130, various NIST Special Publications, and several EPA Directives (see Appendix A). We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We reviewed selected NIST self-assessment questions, EPA's system inventory, and selected system security plans. In addition, we reviewed and tested authentication/identification controls at selected locations. The sampling methodologies provided coverage of EPA's program offices, as well as different types of Agency data (e.g., financial,

enforcement/compliance, and systems containing environmental data). Further details on audit scope and methodology are included in Appendix A.

Prior Audit Coverage

EPA OIG Report No. 2003-P-00009, *EPA Undertaking Implementation Activities to Protect Critical Cyber-Based Infrastructures, Further Steps Needed*, dated March 27, 2003: This report focused on the adequacy of EPA activities for protecting its IT infrastructure and, among other things, recommended that EPA revise security plans for IT systems critical to its cyber-based infrastructure so that they meet NIST requirements.

EPA OIG Report No. 2002-S-00017, *Government Information Security Reform Act: Status of EPA Computer Security Program*, dated September 16, 2002: This report noted that while EPA has made progress in strengthening its security program, management must continue to seek improvements in the areas of risk assessments, effective oversight processes, and training employees with significant security responsibilities.

Chapter 2
Security Self-Assessments Contain Unreliable Data

Our review of selected critical self-assessment responses identified 36 percent that were inaccurate or unsupported. As a consequence, the responses to the self-assessment questions we reviewed did not identify or support the current security status of those systems. The inaccurate responses occurred because OEI issued *Guidance for Reviewing ASSERT Responses to GISRA-related Questions* that was not consistent with NIST guidance. In addition, OEI did not systematically monitor or evaluate the system owner responses to verify the responses were accurate or supported.

Results of Review

Thirty-six percent (78 of 216) of the critical self-assessment questions we examined were inaccurate or unsupported. Approximately 9 percent of system owners responses were inaccurate, and 27 percent were unsupported. We determined a response to be "inaccurate" if the system owner's supporting documentation was not consistent with the data reported in the system self-assessment. We determined a response to be "unsupported" if the system owner did not provide any documentation. For example:

- Ten of 17 systems owners that responded "implemented" to the question, "Is the contingency plan approved by key affected parties?" did not provide the OIG a copy of an approved contingency plan.

- Nine of 16 systems owners that responded "implemented" to the question, "Does the budget request include the security resources required for the system?" did not provide supporting budget documentation to the OIG.

- Eight of the 27 systems owners did not have supporting documentation for 50 percent or more of their responses.

As a consequence, the responses to the self-assessment questions we reviewed did not identify or support the current security status of those systems. OEI reported to OMB a Plan of Actions and Milestones to correct the system weakness for each question that did not have an "implemented" response. Therefore, our review disclosed that Agency's Plan of Actions and Milestones may not have included all necessary action items due to inaccurate or unsupported responses.

We determined system owners did not provide accurate responses to the self-assessment questionnaire, in part, because OEI's guidance to system owners was inconsistent with NIST guidance. For example, in the question "Has a

contingency plan been developed and tested?" OEI's guidance directed the system owner to respond "implemented" as long as the system had a contingency plan in place. Although some system owners had developed a contingency plan, we determined that most plans had not been tested. To be consistent with NIST guidance, these system owners should have responded "procedures" rather than "implemented" to this question. We conferred with the author of NIST 800-26 regarding interpretation of this question and confirmed that system owners only should respond "implemented" when the system contingency plan has been tested.

Another self-assessment question asked, "Are tests and examinations of key controls routinely made, e.g., network scans, analyses of router and switch settings, penetration testing?" OEI guidance directed the system owner to respond "implemented" if the system is subjected to routine monitoring by one of the Agency's automated monitoring tools (Bindview or Enterprise Security Manager). While we agree that the Agency's automated monitoring tools examine technical controls, they do not examine management and operational controls, which should be included in "examination of key controls." NIST confirmed this question includes routinely testing management, operational, and technical controls.

Furthermore, some system owners relied upon statements from system operators or other individuals to formulate responses without obtaining or maintaining documentation to support the veracity of each response. For example, many of the system owners that responded "implemented" to the question "Is the system security plan approved by key affected parties and management?" could not produce a copy of the approved security plan. These system owners could not support the "implemented" response. Also, 2 of the 27 system owners did not respond to the OIG's repeated requests for support documents.

While OEI has performed a variety of monitoring security activities, these activities did not include the systematic monitoring and evaluation of the self-assessment responses. OEI believes the accuracy of the self-assessments is first and foremost the responsibility of the senior agency official who owns the system(s). While we agree that the assigned senior agency official has a responsibility for providing accurate information concerning the system's security controls, FISMA 3544 (3) states "the head of each agency shall delegate to the agency Chief Information Officer the authority to ensure compliance with the requirements imposed on the agency," including designating a senior agency information security officer who shall head an office with the mission and resources to assist in ensuring agency compliance. In our opinion, "ensuring agency compliance" should include systematic monitoring and evaluation of the security self-assessment responses, since such oversight activities will help ensure that the Agency's quarterly report to OMB accurately reflects the effectiveness of EPA's information security program.

Recommendations

We recommend that the Director for Technology, Operations, and Planning:

2-1. Direct system owners to use NIST 800-26 to answer the security control objectives listed in ASSERT or ensure additionally issued guidance is consistent with NIST 800-26.

2-2. Direct system owners to obtain and maintain the documentation to support self-assessment responses and provide such documentation to the OIG upon request.

2-3. Develop and implement a program that systematically monitors and evaluates the system security self-assessment responses.

Agency Comments and OIG Evaluation

In a memorandum dated July 15, 2003, OEI's Director for Technical Information Security responded to our draft report (see Appendix B). In summary, OEI concurred with the report recommendations, but raised concerns regarding the breadth of some finding statements. We modified the report language to clarify that the findings pertained to the critical self-assessment questions and responses we reviewed. We also amended the report to emphasize that we conferred with appropriate NIST personnel, who concurred with our interpretation of their guidance related to self-assessment questions on contingency plans and testing of key controls. In responding to the recommendations, OEI stated it is establishing a procedure under the Agency Network Security Policy to require the use of applicable NIST guidance as the basis of all Agency IT-related policies and procedures. In addition, OEI has dedicated some of its employees to an Agency-wide testing and evaluation program. Subsequent discussions with OEI also resulted in an additional recommendation pertaining to the maintenance of support documentation for security self-assessments. In our view, the corrective actions described in the response are appropriate and should, when fully implemented, respond adequately to the recommendations.

Chapter 3
Systems Inventory Incomplete

ASSERT, EPA's system inventory for security purposes, did not identify all major applications. As a result, not all major applications had a completed security self-assessment, which could impact the overall information security status of the Agency. Although OEI took steps to ensure an accurate inventory of major application systems was obtained, they relied solely on the systems owners to identify which systems met the criteria for a major application or general support system, without systematically evaluating the system owners' responses.

Results of Review

We determined that ASSERT did not include all major applications. OMB requires that all major applications and general support systems be reported under FISMA. FISMA states the head of each Agency shall ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control. In addition, it states the Chief Information Officer will designate a senior agency information security officer who shall head an office with the mission and resources to assist in ensuring agency compliance with FISMA requirements.

We determined an information system to be a major application if it met OMB's definition, as stated in Circular A-130, Appendix III, *Security of Federal Information Resources*. OMB states a "major application" requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. In addition, a "system" can refer to a set of processes, communications, storage, and related resources that are tied together by logical boundaries.

Whether the system includes one application or consists of multiple applications residing on a general support system, NIST stipulates that all applications should be (1) classified as either a major application or general support system, and (2) be covered by a security plan. Finally, NIST states that a security self-assessment should be completed for every major application and general support system.

We found ASSERT did not include the following seven systems that either qualify as major applications or were not included in the self-assessment of one of EPA's general support systems, as shown in Table 2:

Table 2: Systems Not Included in ASSERT		
System Name	**Program Office**	**Explanation**
Asbestos Receivable Tracking System	Office of Chief Financial Officer	Should be a major application. System contains loan receivable information that is confidential in nature.
Inter-Agency Document Online Tracking System	Office of Chief Financial Officer	Should be a major application because data includes confidential business information and has high integrity requirements.
Working Capital Fund Workload and Billing System	Office of Chief Financial Officer	Currently not classified. System should be recognized and accounted for in the security plan and self-assessment of an EPA general support system.
Water Assessment Treatment Results System	Office of Water	Inadvertently deleted from ASSERT 2003, although it was included in prior year inventory.
Bankcard System	Office of Chief Financial Officer	Should be a major application. System must be highly accurate and reliable in order to correctly modify bankcard commitments, create obligations, and prepare payment transactions.
Small Purchase Tracking System	Office of Chief Financial Officer	Should be a major application because of high integrity requirements.
Electronic Approval System	Office of Chief Financial Officer	Currently not classified. System should be recognized and accounted for in the security plan and self-assessment of an EPA general support system.

As a result, not all major applications completed a self-assessment of security controls and related operational practices or were included in the self-assessment for the applicable general support system. Self-assessments provide a method for Agency officials to determine the current status of their information security program and, where necessary, establish a target for improvement. Without a full accounting of major application systems, Agency officials cannot fully understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

Although OEI took steps to obtain an accurate inventory of major application systems, its efforts were not sufficient. For example, in July 2002, OEI sent a memorandum to EPA's Information Security Officers that identified OMB's definitions for general support systems and major applications. In addition, OEI reconciled EPA's inventory to budget documentation, to identify systems that had

not been reported that should have been. Also, OEI instructed Information Security Officers to perform a self-assessment of their respective systems or take action to remove systems that did not meet the criteria of a major application. Despite these actions, major applications were omitted from ASSERT or were not included in the applicable general support system self-assessment. This occurred because OEI relied on systems owners to identify which systems met the criteria for a major application or general support system without systematically evaluating the system owners responses. In addition, the general support system security plan for the Agency's mainframe computer did not include non-major applications that reside on the system.

Recommendations

We recommend that the Director for Technology, Operations, and Planning:

3-1. Direct general support system owners to include all applications residing on the system in the system's security plan.

3-2. Coordinate with system owners to amend ASSERT to add the missing major applications noted in this report.

3-3. Develop and implement a program that systematically monitors and evaluates system classification.

Agency Comments and OIG Evaluation

OEI concurred with the recommendations, and indicated it will (1) coordinate with the system owners to ensure the systems in question are included in the system inventory, unless the system owners can provide adequate documentation to the contrary; and (2) make a diligent effort, under its quality assurance program, to validate that all major applications and general support systems are properly classified and accounted for. Furthermore, our discussions with OEI representatives led to another report recommendation to ensure that general support systems security plans account for all system applications. In our view, the corrective actions described in the response are appropriate and should, when fully implemented, respond adequately to the recommendations.

Chapter 4
Greater Oversight of Authentication/Identification Controls Needed

EPA management did not provide proper oversight to ensure implementation of authentication/identification controls, such as periodic reviews of system access listings to ensure that only authorized individuals have access to each system and that access levels are appropriate. As a result, the potential for unauthorized access, misuse, and system downtime was increased. This occurred because OEI management relied on authentication/identification control information submitted by program and regional offices without validating its reliability.

Results of Review

OEI did not provide sufficient oversight for authentication and identification controls to ensure systems were protected against unauthorized access and misuse. While we recognize that OEI is not directly responsible for implementing authentication/identification controls, the E-Government Act of 2002 charges the senior agency information security officer to head an office with the mission and resources to assist in ensuring agency compliance with FISMA requirements. As such, OEI is accountable for ensuring that EPA's managers implement and maintain appropriate security controls.

We identified program and regional offices that had not properly implemented access controls over selected IT systems. Some system managers did not periodically review access lists to verify that users needed access to the system and that the levels of access were appropriate. For example, periodic reviews of user access lists and users' authorization levels were not conducted on three of the six systems reviewed. As a result, users were assigned greater authorization levels than necessary and some users retained access rights after they no longer required them. These control weaknesses increased the potential for the manipulation and/or misuse of systems.

Also, our examination of user access listings disclosed that Agency systems had not been assigned adequate personnel to ensure the availability of the systems to users, which can increase system downtime. For example, two of the six systems reviewed only empowered one person with the authority to grant or coordinate access for other users. Continued availability is very important for these systems, since their respective security plans state "non-availability of systems or data would impair the Agency's long-term ability to accomplish its mission." These systems are used to support compliance/enforcement-related activities for the national pesticides program.

We are currently drafting a separate report to system owners addressing the system-specific weaknesses we found with regard to user access and authorization levels, maintaining system availability, and the need for more frequent oversight of these authentication/identification controls.

The noted weaknesses occurred, in part, because OEI had not implemented a comprehensive monitoring and evaluation program to ensure system managers comply with established practices governing implementation of controls. Instead, OEI relied on information submitted by the program and regional offices without validating the information. Sufficient oversight for the implementation of authentication/identification controls will help ensure system managers are periodically reviewing user access listings and that the Agency's IT systems are available to users. Furthermore, OEI's oversight of the implementation of security controls will help detect and subsequently assist in preventing unauthorized access and misuse of the Agency's IT systems.

Recommendation

We recommend that the Director for Technology, Operations, and Planning:

4-1. Develop and implement a comprehensive program that systematically monitors and evaluates the implementation of authentication/identification controls.

Agency Comments and OIG Evaluation

OEI's response to the draft report indicated it does not agree that the audit sampling and evaluation methodology supports a broad, Agency-wide conclusion for all technical controls. As such, OEI did not concur with the recommendation. Although the sample was judgmental, we believe the national systems selected provided adequate coverage of EPA's program offices, as well as different types of Agency data (e.g., financial, enforcement/compliance, and systems containing environmental data). However, we modified the report language and recommendation for this chapter, changing "technical controls" to "authentication/identification controls," in order to more specifically reflect the work that was performed.

Chapter 5

Security Plans Not Sufficient

EPA did not adequately address controls in its information system security plans. Our review disclosed that security plans omitted or lacked sufficient details regarding security controls, such as logical access to system data, contingency plans, and planned reviews of system security controls. Systems security plans should comply with NIST guidance by describing controls in place or planned. As a result, management authorized systems to operate without being provided adequate information on the impact that existing risks may have on operations. This weakness occurred, in part, because EPA's security planning guidance had not been revised to include NIST requirements. Also, several system owners used previous security plans that did not comply with NIST as examples to develop or update the current plans.

Results of Review

Our review of selected security plans disclosed that system controls were not adequately planned for in Agency information systems. The system security plans reviewed showed that management, operational, and technical controls were either not included or lacked sufficient details when compared to guidelines found in NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires management to develop security plans that are consistent with NIST guidelines. Furthermore, management's authorization to operate an IT system should be based on an assessment of management, operation, and technical controls, as documented in the system's security plan.

To determine the adequacy of EPA system security plans, we reviewed a judgmental sample of 18 security plans. To ensure we reviewed security plans of systems that are both mission critical and representative of EPA's major financial, administrative, and programmatic systems, we selected our sample from a universe of plans that have benefitted from prior OEI oversight reviews. For each of the security plans reviewed, we evaluated 26 security control elements, defined in NIST 800-18, to ensure each element met the specified level of detail. For example, to meet the level of detail NIST outlined for the "review of security controls," each security plan would need to:

- List any independent security reviews conducted on the system during the last three years.

- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

We summarized our results for each of the 26 major control elements and calculated the percentage of reviewed security plans that were not consistent with NIST guidelines. The following Table 3 identifies those control elements that resulted in the highest percentages of noncompliance with NIST, either because the element was missing from security plans or because the plans did not contain a sufficient level of detail. Additional information on NIST contol elements and our compliance percentages will be made available upon request.

Table 3: Security Plan Reconciliation to NIST 800-18

NIST Control Elements *	Non-compliance
Major Application: Application Software Maintenance Controls ***General Support System:*** Hardware System Software Maintenance Controls	**100%**
Reviews of security controls	**86%**
Identification and Authentication controls	**86%**
Major Application: Data Integrity/Validation Controls ***General Support System:*** Integrity Controls	**85%**
Logical Access Controls	**85%**
Contingency Planning	**79%**
Audit Trails	**79%**
Personnel Security	**79%**
Authorized Processing	**64%**

* For a description of these control elements, see Appendix C.

As a result, management was authorizing systems to operate without being provided adequate information on the impact these risks can have on operations. In addition, a security plan that does not comply with Federal regulations limits management's assurance that the system's owner has identified all applicable security requirements.

These deficiencies occurred because EPA's guidance for developing a system security plan – the Information Security Planning Guidance – had not been revised

since NIST issued guidance on creating a system security plan in 1998. Our review of the Information Security Planning Guidance determined that it does not completely define all key points that NIST 800-18 outlines for inclusion in major application and general support system security plans. For example, EPA's Information Security Planning Guidance does not:

- Require documenting the risk assessment methodology used to identify threats and vulnerabilities.

- Define the level of detail required by NIST for Personnel Security measures pertaining to levels of sensitivity and access.

- Identify general support system requirements for contingency planning.

- Identify the need to develop a security plan for a system at the "initiation phase" of the System Development Life Cycle.

We also found that several system owners used previous security plans, which did not comply with NIST, as examples to update the current plans. In addition, a systematic monitoring and evaluation process was not in place to ensure that security plans met NIST requirements.

Recommendations

We believe that the Agency's Information Security Planning Guidance needs to be revised to align itself with NIST requirements. However, we will not reiterate that need because it is addressed in EPA OIG Report 2003-P-00009, *EPA Undertaking Implementation Activities to Protect Critical Cyber-Based Infrastructures, Further Steps Needed*, dated March 27, 2003.

We recommend that the Director for Technology, Operations, and Planning:

5-1. Establish a completion date as to when all EPA systems security plans will be revised to comply with security plan controls defined in NIST 800-18 guidance, and ensure individual security plans are revised as scheduled.

5-2. Establish a process which systematically monitors and evaluates systems security plans to ensure they comply with NIST guidelines.

Agency Comments and OIG Evaluation

In its response to the draft report, OEI concurred with our initial recommendation but took exception to how the results of our review were presented in Table 3. We modified the report to clarify that Table 3 identifies security plan elements that, based on our review, resulted in the highest percentages of noncompliance with NIST guidelines. Based on subsequent discussions with OEI representatives, we have included an additional recommendation for establishing a process to ensure systems' security plans comply with NIST guidelines. OEI's response indicated that it has formally adopted NIST 800-18 as the basis for Agency security plans. Moreover, it will give priority to ensuring that new system security plans and major revisions to existing plans are consistent with NIST. Per discussion with OEI management, the remaining security plans will be revised in accordance with the established three year review cycle. In our opinion, the planned corrective actions are appropriate.

Appendix A

Details on Scope and Methodology

To accomplish this audit's objectives, we used a variety of Federal and Agency regulatory documents, including:

- A-130, Appendix III, *Security of Federal Automated Information Resources*,
- NIST Special Publications:
  - 800-14, *Principles and Practices for Securing IT Systems*
  - 800-18, *Guide for Developing Security Plans for Information Technology Systems*
  - 800-26, *Security Self-Assessment Guide for Information Technology Systems*
  - 800-30, *Risk Management Guide for Information Technology Systems*
- EPA Directive 2195 A1, *Information Security Manual*
- EPA Directive 2195.1 A4, *Agency Network Security Policy*
- EPA's *Information Security Planning Guidance*

The focus of this audit was to review EPA's policies, procedures, and practices regarding systems' security self-assessments completed during fiscal 2002. We analyzed various supporting documentation and technical controls, and interviewed key EPA personnel. The specific methodology for reviewing and validating self-assessment data, EPA's system inventory, authentication/identification controls, and security plans, follows:

Self-Assessment Data

To determine whether the self-assessments were accurate and supported, we randomly selected a sample of systems from the Agency's ASSERT system, dated November 6, 2002. Specifically, we reviewed system self-assessment responses for eight critical questions, selected by OEI, to determine whether those responses were accurate and supportable. During fiscal 2002, OEI provided system owners additional guidance on how to respond to these eight questions, and we took that additional guidance into account. We reviewed the system owners' responses for 27 systems to determine whether the self-assessment responses were adequately supported. We determined a response to be "inaccurate" if the system owner's supporting documentation was not consistent with the data in the self-assessments and "unsupportable" if the system owners did not provide any documentation.

System Inventory

To determine whether all major applications were listed on EPA's inventory, we reviewed EPA's Enterprise Architecture and reconciled the systems listed to the major applications listed in ASSERT. In addition we reconciled ASSERT to the systems reported as major applications in EPA's 2002 budget submission to OMB (i.e., OMB Exhibits 53 and 300B). For those systems we could not reconcile, we reviewed some Memorandums of Understanding between the offices responsible for the systems and interviewed EPA personnel to determine whether these systems

met the criteria of a major application. In addition, we discussed interpretation of NIST 800-26 with NIST personnel.

Authentication/Identification Controls

We judgmentally sampled six national systems from the universe of major applications listed in ASSERT. The systems selected provided coverage of EPA's program offices, as well as different types of Agency data (e.g., financial, enforcement/compliance, and systems containing environmental data). We reviewed these systems at five regional locations to determine whether authentication/identification controls were implemented. We performed testing to determine whether selected major application systems had adequate authentication and identification techniques, as defined by NIST 800-26. Furthermore, we verified that users listed on the access listing still needed access, and tested their respective levels of access to ensure they were appropriate. Also, we reviewed systems coordinator/administrator listings to determine whether adequate personnel had been assigned to ensure the availability of the systems to users.

Security Plans

We judgmentally selected a sample of 18 security plans from the universe of plans OEI used to conduct its 2002 "completeness review." We evaluated the systems security plans' contents to ensure they included and met the required level of detail described in NIST 800-18. Additionally, we reviewed the Agency's Information Security Planning Guidance to determine whether the guidance defined all key points contained in NIST 800-18.

Agency Response to Draft Report

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
ENVIRONMENTAL INFORMATION

12 / 5 2003

MEMORANDUM

SUBJECT: OEI Response to the Draft Audit Report: *EPA's Computer Security Self-Assessment Process Needs Improvement* Assignment No. 2003-000047

FROM: George Bonina
Director, Technical Information Security Staff (2831T)
and Senior Agency Information Technology Security Officer

TO: Melissa Heist
Assistant Inspector General for Audit (2421T)
Office of the Inspector General

Thank you for the opportunity to review the audit report, *EPA's Computer Security Self-Assessment Process Needs Improvement,* Assignment No. 2003-000047. Mark Day has delegated to me the responsibility for responding to the audit. Attached, you will find a summary of OEI's comments (Attachment 1) and detailed comments included in a mark-up of the draft audit report (Attachment 2). Consistent with your request, we have reviewed the draft audit for factual accuracy and indicated our concurrence or nonconcurrence on the draft findings and recommendations contained therein.

Your analysis of the Agency's self assessment process has highlighted areas that require additional focus and attention by OEI. The detailed analysis of the self assessments will help OEI identify where systems owners' understanding of security program requirements is incomplete and where additional guidance is needed. Your review also serves to reinforce to the programs the seriousness of the process, making it more than just a paper exercise. Given the newness and the complexity of the NIST 800-26 methodology, it is not surprising that system owners experienced some learning pains as they completed their first ever self assessments. As the Agency and system owners become more familiar with this annual process and methodology, OEI anticipates substantial improvement in the self-assessment result.

Despite this valuable analysis of the Agency's security self assessment work, we have a number of concerns that we believe should be addressed to ensure the report's credibility and usefulness to OEI and to the Agency. These concerns, which are described in detail in the attachments, concern the overall tone of the report, the methodology used to draw generalized Agency-wide conclusions and the OIG's interpretation of OMB directives, NIST guidance and FISMA responsibilities.

OEI appreciates the opportunity to provide comments on the draft audit. We are very anxious to work with you to ensure the effectiveness of the Agency's information security program through audits and evaluations. The combination of OIG independent evaluations and CIO implementation and oversight, as envisioned by FISMA and OMB guidance, will keep EPA in the forefront of Federal IT security. We believe that resolution of the issues raised by this audit will strengthen both our roles.

Please feel free to contact me (202-566-0304) to discuss any of our comments in more detail.

cc: Patricia Hill, Director of Business Systems, Office of Inspector General
Mark Day, Director, Office of Technology Operations and Planning

Attachment 1
Summary of OEI Comments on Draft Audit Report, *EPA's Computer Security Self-Assessment Process Needs Improvement* Assignment No. 2003-000047
July 11, 2003

- OEI is concerned about the overall tone of the report. While, there are multiple ways to analyze, interpret and present findings, the report shows the Agency's security program in a poor light that we believe is inconsistent with the actual status of the program. For example, the table titled, "Security Plan Reconcilation to NIST 800-18" presents a "Rate of Deficiency" that implies that virtually all EPA's security plans are so defective as to present a serious security risk to the Agency. In some cases there is the implication of mismanagement by OEI or Agency program officials. For example, the report states that "EPA management directed system owners to respond incorrectly to the self-assessment questions because they misinterpreted NIST's guidance."

- OEI is concerned about the report's use of sweeping, broad generalizations that characterize a number of the findings. The report identifies specific weaknesses in very specific areas and generalizes those findings across the Agency security program. There are four findings which are of particular concern to OEI.

  1-1 OEI does not agree with the unqualified general conclusion that the 2002 GISRA results reported to OMB were based on unreliable data and may not accurately represent the status of EPA's information security program.

  For EPA's information security program to be effective, it is e ssential for program officials to be able to support their assessments. OEI requested the OIG to conduct an audit in this area and appreciates the OIG's positive response to this request. We are concerned that some system managers were not able to provide supporting documentation and we intend to follow-up on this finding. However, OEI's review of the OIG's data concludes that of the eight questions reviewed by the OIG, there are only two questions where the programs' ability to provide adequate supporting documentation is in question. OEI believes that an unqualified Agency-wide finding that questions the validity of EPA's 2002 GISRA submission is unwarranted. The details of OEI's analysis are covered in Attachment 2.

  1-2 In some cases the report uses a "judgmental" sample to form the basis of Agency-wide conclusions. OEI's statistical experts advised us that it is not statistically valid to infer conclusions to the whole population based on the actions of a few judgmentally selected examples. Judgmental samples can only provide insight into the deficiencies of the selected few. Furthermore, OEI believes that the use of judgmental samples for FISMA evaluation purposes is inappropriate. FISMA section 3545(a)(2)(A) states that OIG evaluations should be based on "a <u>representative</u> subset of the Agency's information systems."

  1-3 The report finds that an Agency-wide deficiency exists in the implementation of technical controls on systems. It appears the audit reviewed only identification and authentication controls (not <u>all</u> technical controls as implied by the finding) of a judgmental sample of systems. It also appears that no actual testing of the effectiveness of controls was performed. Instead, the evaluation appears to have consisted of interviews and a review of documentation. OEI believes that this methodology does not support the Agency-wide finding in the report.

  1-4 The report finds that EPA did not adequately plan system controls because EPA's security planning guidance has not been revised to include NIST requirements. OEI believes that this finding is not supportable for two reasons. First, it is based on a judgmental sample of systems. Second, OEI believes that EPA's security planning, consisting of policy and guidance, has been substantially consistent with NIST guidance. There has never been a demonstration that the differences between EPA and NIST guidance were so substantial that there was a significant risk to the Agency's systems.

- OEI and the OIG have differences regarding the interpretation of some of the security mandates in the OMB directives and NIST guidance. Our differences are noted in OEI's comments in Attachment 2. OEI recognizes that the OIG may have legitimate different interpretations of guidance. Those differences should be noted in any audit. However, OEI believes that differences of opinion about how to interpret guidance do not support a finding that questions the reliability of EPA's report to OMB unless the OIG can demonstrate that OEI's guidance was unreasonable and resulted in a substantial risk increase to the Agency.

- The report does not appear to recognize how accountability and responsibility are assigned in FISMA and OMB A-130. Frequently, the report places responsibility on OEI or the CIO for actions that FISMA and OMB A-130 clearly assign to program officials. An example is the finding that OEI is responsible for those systems that were not reported in 2002, despite the fact that OEI provided clear guidance to the programs and made a diligent effort to identify all Agency systems. The non-reported systems were, in fact, determined by the program officials to be not reportable and OEI accordingly accepted their determination. OEI disagrees with the report's finding that there is a systemic problem with system identification that is OEI's responsibility to remedy.

- Throughout the report OEI is criticized for not validating the information provided by the programs. OEI recognizes that it has a responsibility for ensuring effective implementation of the security program and OEI intends to increase its oversight activities. However, the report holds OEI fully accountable for any misreporting by program officials. Under FISMA program officials are responsible for security of the systems under their control and the OIG also has a substantial role in validation. The June 12, 2003 information request from Congressman Putnam to the Inspector General clearly expects that the OIG will play a significant role in validating FISMA 2003 data.

Attachment 2
Expanded OEI Comment on Draft Audit Report, *EPA's Computer Security Self-Assessment Process Needs Improvement* Assignment No. 2003-000047

September 22, 2003

OEI has informally provided the OIG staff with a marked-up version of the report containing comments for their consideration. However OEI is formally submitting the following expanded comment.

Chapter 2

OEI Comment:

For EPA's information security program to be effective, it is essential for program officials to be able to support their assessments. OEI requested the OIG to conduct an audit in this area and appreciates the OIG's positive response to this request. We are concerned that some system managers were not able to provide supporting documentation and we intend to follow-up on this finding. However, OEI's review of the OIG's data concludes that of the eight questions reviewed by the OIG, there are only two questions where the programs' ability to provide adequate supporting documentation is in question. OEI believes that an unqualified Agency-wide finding that questions the validity of EPA's 2002 GISRA submission is unwarranted.

For three of questions dealing with security planning (12.2.1, 5.2.1, 4.1.5), the OIG found that over 90 percent of the systems reviewed were able to provide supporting documentation. For two questions dealing with contingency planning (4.1.4, 9.2.1), OEI disagrees with the OIG interpretation of NIST guidance. OEI believes that it provided the programs with consistent and correct guidance and that OEI accurately reported the status of contingency planning to OMB. OEI, in fact, reported that contingency planning is a problem with only 56 percent of the Agency systems having implemented contingency plans and only 18 percent having tested contingency plans. While the OIG and OEI may disagree on how to characterize the issue, we appear to agree that contingency planning is a weakness that results in a "red" score on the Agency's internal security report card.

For the question regarding testing of controls (2.1.4), OEI disagrees with the OIG's interpretation of NIST guidance and believes that the Agency accurately reported the status of testing of controls to OMB. OEI in fact, reported that only 64% of EPA's had tested controls, resulting in a "red" score on the Agency's internal security report card. Again, while the OIG and OEI disagree on how to characterize the issue, we appear to agree that testing of controls is a weakness for the Agency that needs further improvement.

The remaining two questions with low supporting scores deal with security plan approval (5.1.1) and budget (3.1.5). We believe that an unqualified finding of inaccurate reporting is unwarranted and we should focus on understanding and correcting the underlying reasons for lack of supporting documentation. Some reasons include system owners simply not responding, system owners not understanding the guidance, system owners not having the documentation, the OIG finding the documentation inadequate, or underlying interpretation differences between OEI and OIG.

OIG Recommendation:

2-1. Direct system owners to use NIST guidance to answer the security self-assessment questionnaire.

OEI Comment:

OEI concurs with this recommendation. OEI is establishing a procedure under the Agency Network Security Policy to require the use of applicable NIST guidance as the basis of all Agency IT-related policies and procedures. OEI notes, however, that in some cases, NIST guidance may require interpretation and/or application to EPA's specific situation.

OIG Recommendation:

2-2. Develop and implement a comprehensive quality assurance program that, at a minimum:

- Validates self-assessment responses by sampling systems and responses to determine if the responses are adequately supported.
- Requires system owners to complete a Plan of Actions and Milestones to correct any noted deficiencies.

- Establishes a process to follow up on identified deficiencies and ensure that appropriate corrective actions have been implemented.

OEI Comment:

OEI concurs with this recommendation. OEI is establishing a new Agency-level FMFIA weakness that commits OEI to expanding its Agency-wide testing and evaluation program. Additional FTEs have been transferred into TISS specifically for testing and evaluation. OEI has a well established system for creating and tracking Plans of Actions and Milestones.

Chapter 3

OIG Recommendation:

3-1. Coordinate with system owners to amend EPA's systems inventory to add the seven missing major applications noted in this report.

OEI Comment:

OEI concurs with this recommendation. OEI established clear criteria for systems to be included in the GISRA report and made a diligent effort to identify systems across the Agency. Where system owners determined that certain systems did not meet the criteria, OEI requested documentation of that decision. In further discussions with OIG staff, it has become clear that several of the systems excluded from the systems inventory actually did meet OEI's criteria and should have been included by the system owners. The OIG staff is providing documentation to OEI and OEI will coordinate with the system owners to ensure that the systems in question are included unless the system owners can provide adequate documentation to the contrary.

OIG Recommendation:

3-2. Include in the quality assurance program referred to in Recommendation 2-2 a process to validate that all major IT systems are accounted for on EPA's system inventory.

OEI Comment:

OEI concurs with this recommendation with the understanding that OEI can not guarantee that all major IT systems are actually included in the systems inventory. Under FISMA, the responsibility for categorization of systems is the responsibility of the program official. OEI will make a diligent effort, under its quality assurance program, to validate that all major applications and general support systems are accounted for in the Agency's system inventory. NIST has published a draft Federal Information Processing Standard (FIPS PUB 199) as required under FISMA that establishes standards for system security categorization. Once the FIPS 199 is finalized, OEI plans to re-evaluate its criteria and process for determining system security categorization.

Chapter 4

OEI Comment:

OEI does not agree that the audit methodology supports the conclusion that OEI did not provide proper oversight to ensure implementation of technical security controls. We base this comment on the following:

1. The audit report states that the sample used to make this determination was six systems that were judgmentally selected.
2. Only identification and authentication controls, which are a subset of technical controls, were evaluated.
3. It is not clear from the audit report that any actual testing was performed.

OEI believes that a small judgmental sample, combined with evaluation of only a subset of technical controls does not support a broad Agency-wide conclusion for all technical controls.

OIG Recommendation:

4-1. Ensure system owners strengthen technical controls by tracking identified deficiencies in a Plan of Actions and Milestones.

OEI Comment:

OEI does not concur with this recommendation for the reasons stated above.

Chapter 5

OEI Comment:

OEI does not agree with how the information is presented in the Table, "Security Plan Reconciliation to NIST 800-18." The table implies that EPA's security plans are so deficient as to present a significant security risk to the Agency. The table appears to actually represent the percentage of those plans reviewed that contained a deficiency. OEI believes that the Agency has had effective information security planning guidance that meets the requirements of OMB A-130, Appendix III. This guidance, when properly followed, has resulted in good security plans. In addition, OEI has done a considerable amount of work with owners of CPIC systems to upgrade the quality of their security plans.

OIG Recommendation:

5-1. Establish a Plan of Actions and Milestones, including an estimated completion date, as to when all EPA systems security plans will be revised to comply with NIST 800-18 requirements.

OEI Comment:

While OEI does not agree with the basis for this recommendation as described in the audit report, OEI does concur with the recommendation that NIST 800-18 should be the basis for Agency information security plans. OEI has formally adopted NIST 800-18 as the basis for Agency security plans. All new security plans and major revisions to existing security plans must be consistent with NIST 800-18.

Appendix C

NIST Control Elements

Application Software Maintenance Controls - used to monitor the installation of, and updates to, application software to ensure that the software functions as expected and that a historical record is maintained of application changes.

Hardware System Software Maintenance Controls - used to monitor the installation of and updates to hardware, operating system software, and other software to ensure that the hardware and software function as expected and that a historical record is maintained of application changes.

Review of Security Controls - an independent security review, assessment, or evaluation of the system security controls.

Identification and Authentication Controls - technical measures that prevent unauthorized people (or unauthorized processes) from entering an IT system.

Data Integrity/Validation Controls - used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality.

Integrity Controls - used to protect the operating system, applications, and information in the system from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality.

Logical Access Controls - system-based mechanisms used to specify who or what is to have access to a specific system resource and the type of access that is permitted.

Contingency Planning - procedures that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable.

Audit Trails - a record of system activity by system or application processes and by user activity.

Personnel Security - policies and procedures implemented and executed by people to prevent disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., background screening, procedures to terminate users access).

Authorized Processing - the authorization granted by a management official for a system to process information.

Appendix D

Distribution

Director, Office of Technology, Operations, and Planning (2831T)
Director, Office of Technology, Operations, and Planning/Technical Information Security Staff (2831T)
Comptroller (2731A)
Agency Followup Official (the CFO) (2710A)
Agency Audit Followup Coordinator (2724)
Audit Follow-up Coordinator, Office of Environmental Information (2811R)
Audit Liaison, Office of Environmental Information (2812A)
Inspector General (2410)