OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

EPA Could Improve Its Information Security by Strengthening Verification and Validation Processes

Report No. 2006-P-00002

October 17, 2005

Report Contributors:

Rudolph M. Brevard
Charles Dade
Cheryl Reid
Jefferson Gilkeson
Scott Sammons

Abbreviations

ASSERT	Automated Security Self-Evaluation and Remediation Tracking
EPA	Environmental Protection Agency
C&A	Certification and Accreditation
FISMA	Federal Information Security Management Act
NIST	National Institute for Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&Ms	Plans of Action and Milestones

U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00002
October 17, 2005

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

The Federal Information Security Management Act (FISMA) requires the Office of Inspector General to perform an independent evaluation of the Environmental Protection Agency's (EPA) information security program and practices.

Background

We selected a sample of the EPA's major applications and evaluated:

- certification and accreditation practices;
- system contingency plans; and
- program offices' processes to test and evaluate security controls, including conducting vulnerability tests for known security threats.

For further information, contact our Office of Congressional and Public Liaison at (202) 566-2391.

To view the full report, click on the following link:

www.epa.gov/oig/reports/2006/20051017-2006-P-00002.pdf

EPA Could Improve Its Information Security by Strengthening Verification and Validation Processes

What We Found

Program offices had not effectively implemented processes to comply with Federal and EPA requirements related to information security. We found major applications without: (1) adequate certification and accreditation, (2) contingency plans or testing of the plans, and (3) a process to monitor for known security vulnerabilities. As such, all security control deficiencies are not reported in EPA's Plans of Action and Milestones system. EPA could have discovered these security deficiencies had it implemented processes to verify and validate offices' compliance with established Federal and Agency requirements. Therefore, the Chief Information Officer is not receiving timely and accurate information with which to plan, implement, evaluate, and report its Information Technology security status and security remediation activities to Office of Management and Budget.

What We Recommend

We made four recommendations to the Director of EPA's Office of Technology Operations and Planning. These involved: (1) developing and implementing an ongoing oversight process to review major applications and related general support systems for compliance with Federal and Agency requirements; (2) developing and implementing processes to evaluate the effectiveness of Independent Verification and Validation reviews; (3) developing a strategy for reporting Independent Verification and Validation results to inform Assistant and Regional Administrators on the status of their security programs; and (4) ensuring program offices establish Plans of Action and Milestones for all program office-specific deficiencies identified in subsequent reports related to this review.

The Agency found the report to be an accurate reflection of the Agency security program and concurred with the findings and recommendations.

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

OFFICE OF
INSPECTOR GENERAL

October 17, 2005

MEMORANDUM

SUBJECT: EPA Could Improve Its Information Security by Strengthening
Verification and Validation Processes
Report No. 2006-P-00002

FROM: Rudolph M. Brevard /s/
Acting Director, Business Systems Audits

TO: Kimberly T. Nelson
Assistant Administrator for Environmental Information
and Chief Information Officer

This is our final report on the information security controls audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This audit report contains findings that describe problems the OIG has identified and corrective actions the OIG recommends. This audit report represents the opinion of the OIG, and the findings in this audit report do not necessarily represent the final EPA position. EPA managers, in accordance with established EPA audit resolution procedures, will make final determinations on matters in this audit report.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report 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 further release of this report to the public. For your convenience, this report will be available at http://www.epa.gov/oig.

If you or your staff has any questions regarding this report, please contact me at (202) 566-0893, or Charles Dade, Assignment Manager, at (202) 566-2575.

cc: Mark Day, Director, Office of Technology Operations and Planning

Table of Contents

At a Glance

Chapters

1 Introduction **1**

Purpose 1
Background 2
Scope and Methodology.. 2

2 EPA Could Improve Security Controls Reporting and Compliance by Strengthening Verification and Validation Processes.. 4

Plans of Action and Milestones Did Not Reflect Applications' Security Status.. 4
Application Certification and Accreditation Did Not Meet Guidelines 5
Contingency Planning Practices Had Deficiencies....................................... 6
Testing and Evaluation of Security Controls Needs Improvement…………… 7
EPA Has Not Implemented Adequate Verification and Validation Processes for Systems' Security Controls.. 8
EPA is Taking Steps to Improve Security Compliance Processes 8
Recommendations……………………………………………………………… 9
Agency Comments and OIG Evaluation ……………………………………… 9

Appendices

A Detailed Scope and Methodology... 10

B Federal and Agency Criteria.. 13

C Agency Response to Draft Report………………………………………………… 15

D Distribution ……………………….. 17

Chapter 1
Introduction

Purpose

We audited the Environmental Protection Agency's (EPA) information security program and practices. We selected five major applications from EPA's fiscal 2005 business cases submitted to the Office of Management and Budget (OMB). See Appendix A for a listing of the major applications. We evaluated whether the program office for each selected application:

- complied with Federal and Agency requirements on certification and accreditation (C&A) practices;
- complied with Federal and Agency requirements on contingency plans; and
- implemented processes to test and evaluate security controls, which included conducting vulnerability tests for known security threats.

In addition, we evaluated the following additional security control areas. We have reported the results from the first two areas in our fiscal 2005 Federal Information Security Management Act (FISMA) report template submitted to OMB:[1]

- hardware and Operating Systems configuration,
- security training adequacy for Information Security Officials and System Administrators, and
- program office expenditures of security control funds.

We will also provide results to each program office in separate reports. This report provides the Office of Environmental Information with our findings on information security controls, including deficiencies that require EPA Plans of Action and Milestones (POA&Ms).

[1] Report No. 2006-S-00001, *Fiscal Year 2005 Federal Information Security Management Act Report*, October 3, 2005

Background

Enacted into law on December 17, 2002, as Title III of the E-Government Act of 2002, FISMA defines specific information security requirements Federal agencies must satisfy and assigns responsibilities to agency heads, senior agency officials, and agency inspectors general for satisfying FISMA requirements. FISMA requires that agencies develop policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional impairment of agency information assets.

EPA's Chief Information Officer is responsible for developing and overseeing Agency-wide, risk-based, and cost-effective policies and procedures for addressing information security. Senior Agency officials within EPA's program and regional offices are responsible for enforcing security policies and procedures by assessing potential risks and implementing operational and technical controls that cost-effectively mitigate identified risks to Agency information assets. Senior Agency officials are also responsible for implementing controls and periodically testing and evaluating information security controls to ensure continued compliance with Agency standards.

When a security control weakness is identified, Agency officials create POA&Ms, which document the planned remediation process. EPA uses a central database, the Automated Security Self-Evaluation and Remediation Tracking (ASSERT) tool, to centrally track remediation of weaknesses associated with Information Technology systems. ASSERT serves as the Agency's official record for POA&Ms activity. The Agency reports POA&Ms activity to OMB quarterly.

Scope and Methodology

We conducted our field work from March 2005 to July 2005 at EPA Headquarters in Washington, DC; the National Computer Center, Research Triangle Park, North Carolina; and EPA's Region 3 in Philadelphia, Pennsylvania. We interviewed Agency officials at all locations and contract employees at the National Computer Center. We reviewed application security documentation to determine whether it complied with selected requirements. We reviewed system configuration settings and conducted vulnerability testing of servers for known vulnerabilities. Appendix A has detailed information on our sample selection and the specific scope and methodology applied for each security control area. We reviewed relevant Federal and Agency information security requirements, summarized in Appendix B. We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States.

We evaluated the information security practices of five Agency program offices by selecting a major application system within each program office. For each selected application, we evaluated the following security controls:

- Security C&A practices -- We evaluated whether application security plans, risk assessments, and authorizations for operation complied with Federal and Agency requirements.

- Application contingency plans -- We evaluated whether application contingency plans complied with Federal and Agency requirements, specifically regarding: (1) general content headings, and (2) the adequacy and frequency of tests performed on each plan.

- Processes used to test and evaluate security controls -- We evaluated three areas of security controls: (1) physical controls, (2) contractor personnel security screening, and (3) system vulnerability monitoring.

There were no pertinent issues that required follow up from prior audit reports.

Chapter 2
EPA Could Improve Security Controls Reporting and Compliance by Strengthening Verification and Validation Processes

EPA's POA&Ms were not consistent with the security controls status of the applications we reviewed. We found major applications without:

- adequate certification and accreditation,
- contingency plans or testing of plans, and
- adequate testing and evaluation of security controls.

EPA could have discovered these inconsistencies if it had implemented verification and validation processes to review program offices' compliance with established Federal and Agency requirements. Without these processes, EPA mission-critical information systems may not be adequately protected against known security vulnerabilities or be available in a timely manner in the event of an emergency or disaster.

Plans of Action and Milestones Did Not Reflect Applications' Security Status

Our review disclosed that, in several cases, program offices did not report POA&Ms information in EPA's ASSERT database. As a result, the Chief Information Officer is not receiving timely, accurate, and complete POA&Ms information with which to plan, implement, evaluate, and report EPA's Information Technology security status and security remediation activities to OMB.

As indicated in Table 1, and discussed in detail in subsequent sections, program offices discovered and reported only 22 percent (4 out of 18) of the security weaknesses we identified in our review.

Table 1. Application Security Deficiencies Identified Compared to Deficiencies Discovered and Reported in EPA's ASSERT Database

Area Reviewed	Number of Identified Security Deficiencies	Number of Deficiencies Reported by POA&Ms in ASSERT
Certification & Accreditation (C&A)	10	2
Contingency Plan	8	2
Total	18	4

Application Certification and Accreditation Did Not Meet Guidelines

Of the five applications we reviewed, none of the selected C&A packages fully complied with Federal or Agency requirements. Certification is a comprehensive assessment of a system's managerial, operational, and technical security controls to determine whether the controls are implemented correctly, operating as intended, and producing the desired outcome. Accreditation is the official management decision to authorize operation of an information system and to explicitly accept the risk to EPA's operations, assets, or personnel. By accrediting an information system, senior Agency officials accept responsibility for the security of the system and are fully accountable for any adverse impacts to the Agency if a breach of security occurs. The C&A package includes documents used by the authorizing official to approve an information system for operation.

Our review focused on whether each major application's: 1) security plan was current, had been approved or re-approved within the last 3 years or after a major system change, and contained accurate system status and application environment information; and 2) C&A package contained a current independent review of controls or a full, formal risk assessment. In addition, we evaluated whether management explicitly authorized/re-authorized the application within the last 3 years or re-authorized the application for operation after a significant change in processing before placing the system back into operation. We found 10 C&A deficiencies in the following areas:

- Four C&A packages with security plan deficiencies:

  - one application operating with an expired security plan,
  - one application operating with a security plan that was not updated when the system underwent major changes, and
  - two applications operating with security plans that did not reflect current application status.

- Three C&A packages with independent review or risk assessment deficiencies:

  - one application operating under an expired risk assessment,
  - one application operating without ever having undergone a risk assessment, and
  - one application not re-assessing risks following a significant change in processing.

- Three C&A packages with authorization to operate deficiencies:

  - one application operating without written authorization,
  - one application operating with an expired authorization, and
  - one application that was not re-authorized after a major modification prior to placement back into production.

Based on our findings, senior Agency officials did not have a reasonable basis for accrediting the applications. EPA places itself at greater risk because it could not be sure that adequate steps have been taken to eliminate or mitigate risks.

Contingency Planning Practices Had Deficiencies

Four of the five applications we reviewed had contingency plan deficiencies. Our review focused on whether the application owners had: 1) developed a contingency plan and included contingency plan general content headings consistent with National Institute for Standards and Technology (NIST) guidelines, and 2) adequately tested the plan and documented the test results. We found eight contingency plan deficiencies in the following areas:

- Four contingency plan development-related deficiencies:

    - two applications operating without a contingency plan, and
    - two applications with contingency plans that were not updated to reflect major changes made to the system.

- Four contingency plan testing-related deficiencies:

    - four applications had not tested their plans due to the lack of a contingency plan, or the contingency plan was not updated when the application underwent major changes.

Program offices had not reported 75 percent (six of eight) of the contingency plan deficiencies identified in our review.

In addition, we reviewed the contingency planning efforts for one application that was widely distributed throughout the EPA's Headquarters, regions, and finance centers. Our review determined that the application's program office had established POA&Ms to manage two security deficiencies. However, over several years, the program office took no action to correct these deficiencies.

An adequately documented and tested contingency plan would enable EPA to recover quickly and effectively following a service disruption or disaster. Lack of a tested contingency plan may cause mission critical systems to not be available in a timely manner in the event of, or just after, an emergency or disaster.

Testing and Evaluation of Security Controls Needs Improvement

While the physical controls for server rooms and contractor background screening procedures were adequate, the process to monitor servers for high-risk vulnerabilities needs improvement.

Physical Controls of Server Rooms and Contractor Background Screening Processes Were Effective

Program offices effectively implemented physical controls for the server rooms we evaluated. In particular, we examined fire, temperature, and physical access controls for each server room we evaluated. We did not assess these controls at the Research Triangle Park campus since these areas are currently under review in another audit. Although we found contractor background security screening processes effective, we identified where EPA could improve its procedures. We will issue a separate memorandum outlining our concerns.

Process for Monitoring Servers for Known Vulnerabilities Could Be Improved

Although we found many of the program offices had implemented processes to monitor system activity by activating system-logging features and assessing system configuration settings, EPA could improve its processes for monitoring servers to detect and correct known vulnerabilities. Our vulnerability tests discovered 130 high-risk vulnerabilities on the servers scanned with our vulnerability scanner. We provided our test results to the appropriate program offices and EPA took immediate actions to remediate the risks.

EPA has not implemented monitoring for 21 percent (6 of 29) of the reviewed servers. Table 2 compares the number of vulnerabilities discovered on monitored versus unmonitored servers, as well as the average number of vulnerabilities per server. As noted, unmonitored servers had, on average, 72 percent more vulnerabilities than monitored servers.

Table 2. Vulnerabilities Discovered for Monitored Versus Unmonitored Servers

	Number of Servers	Number of Discovered Vulnerabilities	Average Number of Vulnerabilities per Server
Monitored	23	90	**3.9**
Unmonitored	6	40	**6.7**
Total	29	130	**-**

Routine tests of systems to verify that the security settings are configured correctly, according to established policies, is widely recognized as a preventive step that could reduce security incidences from occurring. Without processes to monitor servers, EPA mission-critical information systems may not be adequately protected against known security vulnerabilities. Exploiting these vulnerabilities could have a serious or severe adverse effect on EPA operations, assets, or individuals.

EPA Has Not Implemented Adequate Verification and Validation Processes for Systems' Security Controls

EPA had not established an ongoing process to review major applications for compliance with Federal and Agency requirements. In December 2002, EPA outlined a thorough process to conduct Independent Verification and Validation of annual system security self-assessments and POA&Ms. However, EPA had not taken steps to conduct activities or commit resources to ensure completion of many of the actions outlined in the "Security Oversight Processes" manual.

Information systems also go through limited security compliance reviews during EPA's Capital Planning and Investment Control process, but these reviews have not successfully identified security control weaknesses. EPA designed its Capital Planning and Investment Control process to analyze, track, and evaluate the risks and results of all major capital investments for information systems. However, the review process was not effective in identifying security weaknesses and ensuring program offices created POA&Ms to report and manage the mitigation of significant security weaknesses.

EPA is Taking Steps to Improve Security Compliance Processes

In subsequent talks, Agency officials indicated that EPA has taken steps to improve its screening of security information contained in business cases. For the fiscal 2007 CPIC process, EPA reassigned this function from contractor support to Technical Information Security Staff. However, the process may be insufficient because Agency officials indicated the process does not require Technical Information Security Staff to:

- review the supporting documentation for the business case's security information,
- conduct tests to independently verify and validate the business case's security status, or
- verify and validate security requirements for systems that are not required to submit a business case – EPA's CPIC Lite submissions.

EPA is also taking further steps to enhance its Independent Verification and Validation practices. Agency officials indicated that Technical Information Security Staff committed resources to increase Independent Verification and

Validation activities. EPA provided our office with notification memorandums outlining planned security reviews to begin in July 2005. EPA's memorandums indicate Technical Information Security Staff will verify and validate a sample of systems' security plans, POA&Ms, and subsections of the systems' self-assessments.

Recommendations

We recommend that the Director, Office of Technology Operations and Planning:

1. Develop and implement an ongoing oversight process to verify and validate security controls of major applications and related general support systems for compliance with Federal and Agency standards, and ensure program offices create POA&Ms for all identified weaknesses. The ongoing oversight process should contain:

   a. criteria and processes to monitor and ensure program offices independently assess or reassess new or changed systems prior to authorization/reauthorization to operate - either through the CPIC process or Independent Verification and Validation,

   b. requirements to review a sample of completed POA&Ms, and

   c. requirements to verify that corrective actions effectively corrected identified deficiencies.

2. Develop and implement processes to evaluate the effectiveness of Independent Verification and Validation reviews.

3. Develop a strategy for reporting Independent Verification and Validation results to inform Assistant and Regional Administrators on the status of their security programs.

4. Ensure program offices establish POA&Ms for all program office-specific deficiencies identified in subsequent reports related to this review.

Agency Comments and OIG Evaluation

In general, the Agency found the draft report was an accurate reflection of its security program and concurred with the findings and recommendations, with the exception of the section discussing the Contractor Background Screening Processes. Office of Environmental Information provided the OIG additional information regarding their processes, and we modified the report.

Appendix A

Detailed Scope and Methodology

Application Selection

We initially selected the following six major applications from among EPA's 25 fiscal 2005 business cases submitted to OMB:

System Name	Program Office
Clean Air Markets Division Business Systems (CAMDBS)	Office of Air and Radiation
Integrated Compliance Information System (ICIS)	Office of Enforcement and Compliance Assurance
Comprehensive Environmental Response, Compensation, and Liability Information System (CERCLIS)	Office of Solid Waste and Emergency Response
Safe Drinking Water Information System (SDWIS)	Office of Water
Integrated Contract Management System (ICMS)	Office of Administration and Resources Management
National Geospatial Program (GEO/GIS)	Office of Environmental Information

We chose applications that were in an operational status, represented different Agency program offices, and had the highest budgeted fiscal 2005 costs for application operation and maintenance for each office selected. We eliminated the National Geospatial Program application from our sample because we discovered (after detailed review of the business case and interview with program officials) that this business case was not an actual information system and proceeded to review the remaining five applications against the specified criteria.

We excluded financial applications owned by the Office of the Chief Financial Officer from our sample because this office's applications are currently undergoing review in the financial statement audit, and the OIG will report deficiencies in these applications separately.

Certification and Accreditation

To evaluate application security C&A practices, we reviewed three areas:

- **Application Security Plans** -- For this area we evaluated whether the security plan met the following three criteria:

    - was approved or reapproved within 3 years or after a major application change,
    - accurately reflected the current status of the application, and
    - accurately described the current application environment.

- **Independent Reviews, Audits of Application Security Controls, Application Risk Assessments** -- For this area we evaluated whether EPA had evidence of completing either:

    - a current independent review or audit of security controls, within the previous 3 years or after a major application change, as set forth by Appendix III of OMB Circular A-130 under security controls for major applications; or
    - a full and formal risk assessment at least every 3 years or after a major application change, as specified by the EPA Agency Network Security Manual 2195.1A4.

    Although the C&A process requires both 1) an independent review or audit of security controls and 2) a full and formal risk assessment at least every 3 years, for purposes of our review, we only verified whether the program offices had one or the other.

- **Written Authorizations for Application Operation** -- For this area we evaluated whether EPA had:

    - written authorization for each application prior to placing the application into operation and/or re-authorization for processing at least every 3 years as required by Appendix III of OMB Circular A-130, or
    - written re-authorization for each application prior to placing the application back into operation after "a significant change in processing" as required by Appendix III of OMB Circular A-130.

We interviewed application managers and system security officials to gain an understanding of the current system operating environment and to assess the significance of ongoing changes to the system environment. We evaluated whether security plans, risk assessments, and authorizations were current and whether the actual system operating environment matched the environment described in the application security plan.

Contingency Plans

We evaluated contingency plans, security plans with contingency planning sections, and other documents that are commonly prepared for contingency planning to determine if they complied with the criteria. We specifically reviewed the plans for the broad, overarching subheadings that NIST criteria deems as being part of a complete contingency plan (e.g., Purpose, Applicability, Scope, References/Requirements, Record of Change, System Description, Line of Succession, and Responsibilities). To determine whether program offices tested contingency plans, we requested and reviewed documentation of tests performed within the past year.

Testing of Security Controls

We reviewed physical security measures and processes to monitor servers for known vulnerabilities. To review physical security measures, we examined fire, temperature, and physical access controls to determine if these controls existed for each server room we evaluated. We confirmed the presence of fire suppression systems and alarms. To evaluate server monitoring, we examined documents related to system monitoring and scanning, such as reports from scanning tools and screen prints of system logs; monitoring and configuration applications; and patch management tools associated with each server evaluated. To evaluate contractor background screenings, we obtained documents showing the current status of background screenings for the contractor personnel included within our review.

We used the Internet Security Scanner and NESSUS vulnerability assessment tools to identify computers and open ports susceptible to attack and provide information on the associated vulnerabilities and risk mitigation strategies. The Internet Security Scanner is a network-based vulnerability-scanning tool that identifies security holes on network hosts. NESSUS is a freeware network-based vulnerability-scanning tool that identifies security holes on network hosts. We conducted testing at EPA’s Headquarters, Region 3, and Research Triangle Park. We interviewed responsible system owners and provided results to Agency officials for comments.

Table 2 of our report contains only the *High Risk* vulnerabilities identified by the scanning tools. For password vulnerabilities, we counted one vulnerability per server, although there may have been more than one instance of the same vulnerability. We did not count expired passwords that were under 90 days old as vulnerabilities. We did not report vulnerabilities identified as *Medium* or *Low Risks* or test results described as *Informational.* However, we shared the complete vulnerability test results to the system owners and administrators.

Appendix B

Federal and Agency Criteria

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources requires a management official to accredit (authorize to operate), in writing, the use of an automated system by confirming that its security plan, as implemented, adequately secures the application. The management official must factor in the results of the most recent review or audit of security controls when accrediting the system. The management official must accredit the application prior to its placement into operation and re-accredit the application at least every 3 years, or after major system changes. Major applications must undergo an independent review or audit of the security controls at least every 3 years. The Circular establishes the requirement for all major applications to have security plans.

Federal Information Processing Standards Publication 102, Guideline for Computer Security Certification and Accreditation, September 1983, and NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004. These documents provide guidelines for establishing formal processes for certifying and accrediting computer applications as required by OMB Circular A-130, Appendix III. A security certification consists of an evaluation of an application – including an assessment of the managerial, operational, and technical controls – to see how well these controls meet security requirements. A security accreditation is the official management decision given by a senior Agency official to authorize operation of an information system and to explicitly accept the risk to Agency operations, assets, or personnel based on the implementation of an agreed-upon set of security controls. NIST 800-37 also requires continuous monitoring of system security controls and reporting security status to appropriate Agency officials.

NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, June 2002, maps out guidelines for a complete Information Technology contingency plan as well as testing of the plan. The guidelines specify that contingency plans contain the following sections: Purpose, Applicability, Scope, References/Requirements, Record of Change, System Description, Line of Succession, and Responsibilities. Appendix C states that testing of the contingency plan should occur at least annually and upon significant changes to the Information Technology system, supported business processes, or the Information Technology contingency plan.

EPA Directive 2195A1, EPA Information Security Manual, December 1999, requires each primary organization head to ensure that all general support systems and major applications have security plans in place and update the plan at least every 3 years or when significant change occurs. Appendix A establishes the requirement to develop and test contingency plans.

EPA Order 2195.1 A4, Agency Network Security Policy, March 2001, requires that EPA data communications network resources be documented, monitored, tested, evaluated, and verified to ensure adequate security in accordance with information sensitivity and other Federal and Agency requirements. A program of continuous monitoring, detecting, and auditing with corresponding tracking capabilities and reporting is required for all EPA data communications network entry and exit points. This program must contain procedures for adequate and timely response to intruders and other unauthorized activities. The Order requires major application managers to conduct and update risk assessments at least every 3 years or whenever a substantive configuration change occurs.

EPA Risk Assessment Procedures, February 2004, require system owners to perform a full formal risk assessment on all major applications included in OMB Exhibit 300 submissions before a system is placed in operation and at least every 3 years thereafter.

Appendix C

Agency Response to Draft Report

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

OFFICE OF
ENVIRONMENTAL INFORMATION

September 29, 2005

MEMORANDUM

SUBJECT: Technical Information Security Staff Comments on the Draft Report: EPA Could Improve Its Information Security by Strengthening Verification and Validation Processes,
Assignment No: 2005-000661

FROM: Kimberly T. Nelson */s/*
Assistant Administrator and Chief Information Officer

TO: Nikki L. Tinsley
Inspector General

We appreciate the opportunity to review and provide comments on the Draft Report, "*EPA Could Improve its Information Security by Strengthening Verification and Validation Processes*." Our comments address the factual accuracy of the draft report and include our concurrence or non-concurrence with the findings and recommendations.

In general, we found the report was an accurate reflection of the Agency security program especially in light of our follow-on discussions with your office and the information technology system owners for the systems reviewed. We concur with the findings and recommendations.

If you or your staff have any questions regarding this report, please contact me at 202-566-0304 or Marian Cody at 202-566-0302.

cc: Rudolph Brevard (2421T)
Mark Day (2831T)
Myra Galbreath (2831T)
Karen Maher (2831T)
George Bonina (2831T)
Marian Cody (2831T)
Barbara Chancey (2831T)
John Gibson (N276-01)
Melissa Heist (2421T)
Kim Farmer (2831T)
Bob Trent (2812T)
Cheryl Reid (N283-01)

Appendix D

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Assistant Administrator for Administration and Resources Management
Assistant Administrator for Air and Radiation
Assistant Administrator for Enforcement and Compliance Assurance
Assistant Administrator for Solid Waste and Emergency Response
Assistant Administrator for Water
Director, Office of Technology Operations and Planning
Senior Agency Information Security Officer
Director, National Technology Services Division
Associate Director, Technical Information Security Staff
Operations Security Manager, National Technology Services Division
Audit Coordinator, Office of Environmental Information
Audit Coordinator, Technical Information Security Staff
Audit Coordinator, Office of Administration and Resources Management
Audit Coordinator, Office of Air and Radiation
Audit Coordinator, Office of Enforcement and Compliance Assurance
Audit Coordinator, Office of Solid Waste and Emergency Response
Audit Coordinator, Office of Water
Agency Followup Official (the CFO)
Agency Followup Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Inspector General