U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

Improvements Needed in Key EPA Information System Security Practices

Report No. 10-P-0146

June 15, 2010

Abbreviations

AO	Authorizing Official
ASSERT	Automated System Security Evaluation and Remediation Tracking
CA	Certification Agent
C&A	Certification and Accreditation
CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Management Act
GAO	U.S. Government Accountability Office
IV&V	Independent Verification and Validation
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTOP	Office of Technology Operations and Planning
POA&M	Plan of Actions and Milestones
READ	Registry of EPA's Applications and Databases
TISS	Technology and Information Security Staff

U.S. Environmental Protection Agency
Office of Inspector General

10-P-0146
June 15, 2010

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

The Office of Inspector General contracted with Williams, Adley & Company, LLP, to perform an independent review of the U.S. Environmental Protection Agency's (EPA's) information security program to determine whether it meets the requirements of the Federal Information Security Management Act.

Background

The Federal Information Security Management Act requires inspectors general, or the independent evaluators they choose, to perform an annual evaluation of their agencies' information security programs and practices.

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

To view the full report, click on the following link:
www.epa.gov/oig/reports/2010/20100615-10-P-0146.pdf

Improvements Needed in Key EPA Information System Security Practices

What Williams, Adley & Company, LLP, Found

Williams Adley found that EPA program offices lacked evidence that they planned and executed tests of information system security controls as required by federal requirements. In addition, Williams Adley found that contingency plans developed and maintained by program offices were not current and accurate, and the certification and accreditation process and review of security plans needed improvements. EPA also had two authoritative system inventories that did not reconcile. Finally, EPA had contractor-owned and -operated systems in operation without proper oversight monitoring.

What Williams, Adley & Company, LLP, Recommends

Williams Adley's recommendations to the Director of the Office of Technology Operations and Planning include communicating and training EPA's information security community on testing and documenting information systems security controls. Williams Adley also recommends the Director enhance the quality assurance process to verify that self-assessments evaluate all required security controls.

Williams Adley recommends that the Principal Deputy Assistant Administrator of Environmental Information and Deputy Chief Information Officer direct offices to design and implement a process to perform a periodic reconciliation between its two authoritative system inventories.

Agency officials did not provide comments to the draft audit report and indicated they will provide a response to the final report.

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

OFFICE OF
INSPECTOR GENERAL

June 15, 2010

MEMORANDUM

SUBJECT: Improvements Needed in Key EPA Information System Security Practices
Report No. 10-P-0146

FROM: Rudolph M. Brevard
Director, Information Resources Management Assessments
Office of Mission Systems

TO: Linda A. Travers
Principal Deputy Assistant Administrator for Environmental Information
and Deputy Chief Information Officer

Vaughn Noga
Director, Office of Technology Operations and Planning
Office of Environmental Information

This is the report on the subject audit prepared by Williams, Adley and Company, LLP, on behalf of the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). Williams Adley prepared this report as part of its review of EPA's information security program for Fiscal Year 2009 as required by the Federal Information Security Management Act. This report contains findings that describe the problems Williams Adley identified and corrective actions Williams Adley recommends. This report represents the opinions of Williams Adley and does not necessarily represent the final EPA position. Final determinations of matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The estimated cost of this report – which includes contract costs and OIG's contract management oversight – is $136,242.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report within 90 calendar days. You should include a corrective action plan for agreed-upon

actions, including milestone dates. We have no objections to the further release of this report to the public. This report will be available at http://www.epa.gov/oig.

If you or your staff have any questions regarding this report, please contact me at (202) 566-0893 or brevard.rudy@epa.gov, or Cheryl Reid at (919) 541-2256 or reid.cheryl@epa.gov.

June 15, 2010

MEMORANDUM

SUBJECT: Improvements Needed in Key EPA Information System Security Practices
Report No. 10-P-0146

FROM: Robert J. Fulkerson
Director IT Assurance and Business Solutions
Williams, Adley & Company, LLP

THRU: Rudolph M. Brevard
Director, Information Resources Management Assessments
Office of Inspector General

TO: Linda A. Travers
Principal Deputy Assistant Administrator for Environmental Information
and Deputy Chief Information Officer

This is our final report on the review of the U.S. Environmental Protection Agency's (EPA's) information security program as required by the Federal Information Security Management Act. Williams, Adley & Company LLP conducted this audit on behalf of the EPA Office of Inspector General (OIG). This report outlines weaknesses found and recommendations to correct the noted weaknesses.

We would like to thank your staff for their cooperation throughout the audit process. Please contact the EPA OIG for further information related to this report.

Table of Contents

Appendices

Purpose

As part of the Fiscal Year 2009 Federal Information Security Management Act (FISMA) review, the Office of Inspector General (OIG) tasked Williams, Adley and Company, LLP, to review and assess the U.S. Environmental Protection Agency's (EPA) information security program and annual reporting to the Office of Management and Budget (OMB) on the effectiveness of the information system security program.

Williams Adley conducted this review in accordance with generally accepted government auditing standards. These standards require that Williams Adley plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objectives. Williams Adley believes the evidence obtained provides a reasonable basis for our findings and conclusions.

Appendix A describes the detailed Scope and Methodology of this review.

Noteworthy Achievements

EPA's management officials indicated that they have taken the following actions to improve the Agency's information security program:

- Executed contractual agreements to review all certification and accreditation (C&A) packages.
- Implemented "on-site" training of Agency personnel on preparing C&A system documentation and managing associated plans of actions and milestones (POA&Ms).
- Increased its independent verification and validation activities (IV&V) to review 10 percent of the Agency's information systems.
- Procured an automated C&A tool that will require all C&A artifacts to be published, stored, and maintained within EPA's Automated System Security Evaluation and Remediation Tracking (ASSERT) system.

Findings

Strengthening of managerial controls is needed to ensure delegated information security activities are carried out as intended. EPA delegates implementation of its information security practices to senior managers throughout the Agency. While many offices have practices in place, our review disclosed that personnel with significant security responsibilities continue to face challenges in demonstrating that they executed required tasks. In particular, offices lacked:

- Evidence that testing of information systems security controls took place as required by federal guidance,
- Contingency plan testing on an annual basis,
- Practices to ensure an Authorizing Official (AO) receives credible information to make risk-based decisions, and

- Internal controls to ensure personnel are familiar with their duties and responsibilities for overseeing EPA-owned and contractor-operated systems.

OMB, National Institute of Standards and Technology (NIST), and EPA guidance outline requirements for key information security activities. EPA also implemented a quality assurance program to verify the effectiveness of information security practices. However, in general, EPA offices did not put the emphasis on performing and documenting accomplishment of these critical information security processes. Testing of security controls and continuity plans, and informing AOs about potential threats provide the framework for EPA offices to apply risk mitigation strategies. Without performing these tasks fully, management is not presented with the information needed to make informed decisions about the amount of risks they are willing to assume for continued operations of their network-attached resources and what steps they should take to reduce their risks. Furthermore, without having personnel knowledgeable of their contractor oversight responsibilities, EPA faces the potential that threats to its networked-attached resources could exist without management having the opportunity to mitigate them.

Additionally, our review disclosed that the Office of Environmental Information (OEI) lacked an oversight process to reconcile two databases used to inventory Agency systems and applications. These two databases represent the inventory of known EPA databases and applications. Without reconciling these inventories, management increases the potential that it may not have taken appropriate risk mitigation actions because they were not aware the threat existed. Additionally, prior audit reports highlighted areas of concern with EPA's quality assurance program that management should take steps to correct. Having a quality assurance program that focuses on ensuring security-related activities are designed and executed as intended helps management obtain greater assurance that critical security steps are taking place as management intended.

Documenting Information Systems Security Controls Testing Needs Improvement

EPA program offices were not maintaining documentation that demonstrates testing of security controls was performed as prescribed in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* as follows:

- AO or designated representative determined the required level of independence for security control assessors based on the results of the security categorization process.
- Systems managed by third party service providers were tested independently.
- Certification Agent (CA) certified that the security controls documented in the System Security Planning Package were correct.
- CA notified the Information System Security Officer of the results and recommended changes. (The Information System Security Officer is responsible for updating and maintaining the system documentation.)

Our tests revealed information missing in the documentation:

- The office tested all minimally required security controls as prescribed by NIST within the last three years.

- Tests of systems managed by third party service providers were performed by an independent party as required by NIST.
- System tests were conducted and signed off by multiple individuals. Security documentation for 10 of the 19 systems reviewed showed that the same individual who evaluated the system's security controls also signed off on the test results.

EPA's C&A procedures state that the AO is responsible for operating an information system at an acceptable level of risk to agency, assets, or individuals. As such, the AO determines if the level of independence is sufficient to provide confidence that the assessment results can be used to make a risk-based decision on whether to place the information system into operation or continued operation. Incomplete documentation increases the risks that the AO may authorize the system for processing without adequate knowledge of security weaknesses associated with a critical risk-based decision.

EPA implemented a quality assurance process to review IV&V and C&A reports that program offices generate as a result of system testing. However, these efforts are only applied to new IV&V tests and C&A reports. Therefore, there is limited validation to ensure all EPA systems are tested on a regular basis and oversight activities rely heavily on self-reported information program offices provide. Furthermore, the quality assurance process lacks an emphasis on ensuring that EPA offices plan and execute security testing according to federal guidance because test results and activities are reviewed after they have already occurred. Thereby, the quality assurance process misses the opportunity to ensure that the limited resources dedicated to information systems security are achieving the greatest impact for the Agency.

EPA OIG Report No. 10-P-0058, *Self-reported Data Unreliable for Assessing EPA's Computer Security Program*, February 2, 2010, highlights concerns with EPA's quality assurance program and made recommendations. Taking steps to correct previously reported weaknesses as well as those highlighted in this report should help management gain greater confidence in the security control testing information used for deciding whether to authorize a system for operation.

Contingency Planning Practices Need Improvement

EPA has not established the necessary controls to ensure compliance with NIST requirements and EPA policies for annual testing of contingency plans. Current EPA procedures and processes do not ensure that unsuccessful tests are addressed in a timely manner and all stakeholders are adequately informed of testing results in a timely manner.

For the 19 systems selected for testing, the following observations were noted:

- Contingency plans were not current and have not been fully implemented.
- Documentation did not include testing results and lessons learned.
- Testing plans and procedures did not address the causes for failure.
- Testing plans and results were not signed by AOs.

The lack of a comprehensive contingency plan increases the risks that the Agency may not recover its mission critical systems from a significant disruption to meet its business mission in a

timely manner. According to NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems,* testing should occur at least annually or when significant changes are made to the system, business process, or contingency assumptions. Testing results and lessons learned should be documented and reviewed by participants and other key personnel as appropriate. In addition, the EPA procedural guidelines state that the plan, recovery capabilities, and personnel are tested annually to identify weaknesses.

Review Process for Certification and Accreditation and Security Plans Needs Improvement

EPA needs to improve its quality assurance procedures to ensure C&A documents and security plans are current, properly approved by authorized personnel, and clearly define and delegate authorities. For the 19 systems selected for testing, we identified the following observations of C&A:

- Information System Security Officers did not ensure C&A security documents were current, documented, and authorized in compliance with regulatory requirements.
- Information System Security Officers did not update ASSERT to match current C&A security documents.
- EPA did not provide a signature on contractor C&A supporting documents.

For the 19 system selected for testing, we identified the following observations for the security plans:

- Security roles and responsibilities are not properly defined.
- Delegation memorandums for assigning responsibility are not signed by an authorizing agent.
- Authorization for contractor assignment of responsibility and delegation of authority was not documented and approved.
- A delegation memorandum is not maintained in ASSERT.
- Security plans are not current.
- Points of contacts are not updated in a timely manner.

NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* requires independent certification for systems with a risk category rating of high or moderate. Each phase in the C&A process must consist of well-defined tasks and subtasks that are to be carried out, as indicated, by responsible individuals. Agency officials may appoint appropriately qualified individuals, to include contractors, to perform the activities associated with any security C&A role with the exception of the Chief Information Officer and AO. The only activity that cannot be delegated by the AO is the security accreditation decision and the signing of the associated accreditation decision letter (i.e., the acceptability of risk to the Agency). EPA 2150.0, *Agency Network Security Policy,* requires that general support systems and major applications undergo C&A prior to connecting to EPA networks. Further, the system's C&A expires after three years, or sooner if a major change occurs, and all system interconnections must receive written management authorization based on acceptable levels of risk.

Without documentation that supports and demonstrates security responsibilities and activities are properly carried out, EPA increases the risk that system security controls will not be adequately developed and implemented to effectively address the security risks. These risks include preventing and detecting unauthorized modification of data, unauthorized access to mission critical data, financial data, and personally identifying information.

Contractor Oversight Needs Improvement

EPA had not clearly defined contractor monitoring duties and responsibilities for contractor oversight. Further, EPA had not provided the necessary training to Agency personnel to enable them to perform oversight. For the sample of 19 systems tested, 3 systems were maintained by a contractor. We noted that EPA personnel assigned responsibilities for overseeing contractors were unfamiliar with their duties and documentation requirements. In one instance, the office had not yet assigned monitoring to an EPA official.

Without an effective contractor oversight program, EPA increases the risks that unauthorized activities may occur and go undetected, resulting in loss, destruction, theft, and misuse of sensitive proprietary information. In addition, EPA increases the risk that contractor system security controls implemented by the contractor may not be effective to properly secure and safeguard Agency data.

Practices Used to Identify All EPA Systems Need Improvement

EPA had not performed a reconciliation between EPA's ASSERT and Registry of EPA's Applications and Databases (READ) to identify all reportable systems (see Appendix B for descriptions of ASSERT and READ systems). A review of the ASSERT and READ inventories disclosed a difference of 54 systems. During our analysis, we noted EPA discontinued the inventory reconciliation between the two systems. In addition, the READ Administrator is aware that READ is not current and READ does not:

- Reflect changes to system names.
- Reflect changes to the system status for being reportable.
- Identify reportable systems under development.
- Illustrate the status of retired reportable systems.

Within OEI, the Office of Technology Operations and Planning (OTOP) oversees ASSERT and the Office of Information Collection oversees READ. Annually, the Chief Information Officer requests that senior agency officials enter into READ a comprehensive listing of their information resources. Similar data calls are also made to Agency officials requesting updates to their system information in ASSERT. While EPA makes efforts to maintain the accuracy of both data sources, a lack of coordination between the offices that oversee ASSERT and READ hinders the reconciliation between the two systems.

Without a complete and accurate inventory of all systems, EPA increases the risk that personnel responsible for providing oversight of the Agency's information security program have the information necessary to ensure required security control activities are performed as required by

federal requirements. Also, management may not be informed of the full scope of risks an EPA application poses to the Agency's network so management could make risk-based decisions for mitigating potential threats.

Agency Comments and OIG Evaluation

The Agency declined to provide comments to the draft audit report and indicated responses will be provided for the final audit report.

Recommendations

Williams Adley recommends the Director, Office of Technology Operations and Planning:

1. Issue a memorandum to the EPA information security community that reiterates the requirements for documenting information systems security control testing.
2. Implement training on the appropriate method for documenting tests of information systems security controls and incorporate this training into the Annual Information Security Conference.
3. Enhance the quality assurance process to verify that:
    a. required security controls are evaluated annually as part of the FISMA self-assessment,
    b. security control evaluations are independent and testing results include a documented strategy to resolve all weaknesses,
    c. documentation of security controls testing is complete and adequately supports the objectives,
    d. testing plans and procedures address the cause for testing failures, and
    e. NIST and EPA requirements for security planning, assigning security responsibilities, and maintaining C&A documents (agency's and contractor's) are being followed.
4. Develop and implement a procedure requiring Information System Security Officers submit proposed test plans to the Director of Technology and Information Security Staff (TISS), or request a waiver with justification for eliminating test(s).
5. Require the Director of TISS review and approve information systems security controls test plans prior to the Information System Security Officers conducting tests.
6. Develop an inventory of systems that require contingency plans and maintain the status of updates, test dates, testing results, and resolution required. Create POA&Ms in ASSERT, as needed.
7. Revise the Network Security Policy to enforce the requirements of NIST Special Publication 800-37, regarding responsibilities, delegation of authority, and independence.
8. Design and implement a training program on requirements for monitoring contractor oversight based on EPA roles and responsibilities.

Williams Adley recommends the Principal Deputy Assistant Administrator of Environmental Information and Deputy Chief Information Officer:

9. Direct the Director, OTOP and the Director, Office of Information Collection, to design and implement a process to perform a periodic reconciliation of ASSERT and READ.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed To Amount
1	6	Issue a memorandum to the EPA information security community that reiterates the requirements for documenting information systems security control testing.	O	Director, Office of Technology Operations and Planning			
2	6	Implement training on the appropriate method for documenting tests of information systems security controls and incorporate this training into the Annual Information Security Conference.	O	Director, Office of Technology Operations and Planning			
3	6	Enhance the quality assurance process to verify that: a. required security controls are evaluated annually as part of the FISMA self-assessment, b. security control evaluations are independent and testing results include a documented strategy to resolve all weaknesses, c. documentation of security controls testing is complete and adequately supports the objectives, d. testing plans and procedures address the cause for testing failures, and e. NIST and EPA requirements for security planning, assigning security responsibilities, and maintaining C&A documents (agency's and contractor's) are being followed.	O	Director, Office of Technology Operations and Planning			
4	6	Develop and implement a procedure requiring Information System Security Officers submit proposed test plans to the Director of TISS, or request a waiver with justification for eliminating test(s).	O	Director, Office of Technology Operations and Planning			
5	6	Require the Director of TISS review and approve information systems security controls test plans prior to the Information System Security Officers conducting tests.	O	Director, Office of Technology Operations and Planning			
6	6	Develop an inventory of systems that require contingency plans and maintain the status of updates, test dates, testing results and resolution required. Create a POA&M in ASSERT, as needed.	O	Director, Office of Technology Operations and Planning			
7	6	Revise the Network Security Policy to enforce the requirements of NIST Special Publication 800-37, regarding responsibilities, delegation of authority, and independence.	O	Director, Office of Technology Operations and Planning			
8	6	Design and implement a training program on requirements for monitoring contractor oversight based on EPA roles and responsibilities.	O	Director, Office of Technology Operations and Planning			
9	6	Direct the Director, OTOP and the Director, Office of Information Collection to design and implement a process to perform a periodic reconciliation of ASSERT and READ.	O	Principal Deputy Assistant Administrator of Environmental Information and Deputy Chief Information Officer			

O = recommendation is open with agreed-to corrective actions pending
C = recommendation is closed with all agreed-to actions completed
U = recommendation is undecided with resolution efforts in progress

Appendix A

Scope and Methodology

Williams Adley's review methodology was based on OIG reporting instructions outlined in OMB's Memorandum M-08-21, *Fiscal Year 2009 Reporting Instructions for FISMA and Agency Privacy Management.* Williams Adley re-examined the information and updated the OIG report to address report requirement changes in OMB Memorandum M-09-29 *Fiscal Year 2009 Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management*, August 20, 2009, and OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007.

Williams Adley extracted a sample of 19 systems (16 Agency systems and 3 contractor-owned systems) from ASSERT (as of March 19, 2009) to evaluate the effectiveness of EPA's policies and procedures based on OMB's FISMA fiscal year 2009 reporting instructions. The table below provides descriptive information of each system evaluated.

Table 1: Systems Reviewed For Fiscal Year 2009 FISMA Audit

System Name	*Program Office*	*System Type*	*Risk Category*
Office of the Administrator Local Area Network	Office of the Administrator	Agency	Moderate
APBD\CFO LAN Container	Office of Chief Financial Officer	Agency	Moderate
CINC\OARM	Office of Administration and Resources Management	Agency	Moderate
CIDNET	Office of Enforcement and Compliance Assurance	Agency	Low
Enforcement Action Response System	Region 5	Agency	Low
Contract Laboratory Program Support Systems	Office of Solid Waste and Emergency Response	Agency	Moderate
Enterprise Content Management System	Office of Environmental Information	Agency	Moderate
Integrated Grants Management System	Office of Administration and Resources Management	Agency	Moderate
Inter-Agency Document Online Tracking System	Office of Chief Financial Officer	Agency	Moderate
NAREL LAN	Office of Air and Radiation	Agency	Moderate
NERL-Athens	Office of Research and Development	Agency	Low
NESC Supercomputing	Office of Environmental Information	Agency	Low
OPRM LAN (Shared Services)	Office of Administration and Resources Management	Agency	Moderate
OW/OST LAN Container	Office of Water	Agency	Moderate
Region 8 Libby	Region 8	Agency	Low
Video Teleconferencing Infrastructure	Office of Environmental Information	Agency	Low
Enforcement Support Tracking System	Region 9	Contractor	Moderate
SRA-Verio	Office of Environmental Information	Contractor	Moderate
Working Capital Fund Workload and Billing	Office of Environmental Information	Contractor	Moderate

Source: Williams Adley compilation from EPA ASSERT System Data.

Williams Adley performed the following audit procedures:

- Obtained and reviewed the following FISMA required documents for the 19 systems (Agency and contractor managed/operated systems):
  - certification and accreditation reports.
  - security plans and test reports.
  - contingency plans and tests.
  - risk assessments.

- Obtained and reviewed EPA's:
  - POA&M process and system security categorization for compliance with Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems.*
  - Privacy Program policies and procedures for compliance with federal laws, regulations, and OMB Memorandums M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information and Privacy Impact Assessments.

- Assessed system documentation for compliance with:
  - OMB Circular No. A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources.*
  - NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems.*
  - NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems.*
  - NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems.*

- Reviewed and tested EPA's:
  - Configuration Management processes and procedures.
  - Incident Reporting policies and procedures.

- Reviewed the Agency's Information Security Awareness Training Program to include training on peer–to-peer file sharing.

- Conducted interviews with the Agency's program officials and senior agency officials.

- Conducted internal non-intrusive network vulnerability tests at the following five EPA locations:
  - Headquarters in Washington, DC.
  - Research Triangle Park Finance Center in Durham, North Carolina.
  - National Computer Center in Durham, North Carolina.
  - Region 8 in Denver, Colorado.
  - Great Lakes National Program Office, located at EPA Region 5 in Chicago, Illinois.

Appendix B

Description of ASSERT and Read Systems

Automated System Security Evaluation and Remediation Tracking System (ASSERT)

EPA uses ASSERT, an on-line tool, to gather information regarding testing and evaluation of EPA information assets, track progress of remediation actions, and generate FISMA reports for EPA management. ASSERT currently contains two integrated modules (security self-assessments and remediation tracking) and a third semi-standalone module (system categorization). The ASSERT security assessment module allows Information System Security Officers to enter information to complete their assessment. The remediation module in ASSERT allows Information System Security Officers to enter and update POA&Ms to remediate information technology weaknesses identified.

The system also provides EPA management the ability to monitor activities on-line as updates occur. The module includes an EPA standardized approach for developing POA&M corrective action responses to address in a timely manner the weaknesses discovered during any type of assessment or security review conducted for an Agency information technology asset. ASSERT is EPA's system of record for FISMA reporting.

Registry of EPA's Applications and Databases (READ)

The READ system is a repository for all EPA systems that includes systems reportable to FISMA and non-reportable systems. READ is considered the authoritative source for all EPA information systems. Each information resource (application/system, dataset, or model) is to have a record in READ. The record includes information such as: title, acronym, description, contact information, and organization that owns or operates the system. READ shows the governmental statute supported by the system, life cycle information, and access information.

Appendix C

Distribution

Office of the Administrator
Principal Deputy Assistant Administrator for Environmental Information and Deputy Chief Information Officer
Director, Office of Technology Operations and Planning, Office of Environmental Information
Agency Follow-up Official (the CFO)
Agency Follow-up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Acting Director, Technology and Information Security Staff, Office of Environmental Information
Audit Follow-up Coordinator, Office of Environmental Information
Audit Follow-up Coordinator, Office of Technology Operations and Planning, Office of Environmental Information
Audit Follow-up Coordinator, Technology and Information Security Staff, Office of Environmental Information
Acting Inspector General