U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

*Catalyst for Improving the Environment*

## Briefing Report

# Self-reported Data Unreliable for Assessing EPA's Computer Security Program

**Report No. 10-P-0058**

**February 2, 2010**

**Report Contributors:**

Rudolph M. Brevard
Cheryl Reid
Vincent Campbell
Warren Brooks
Christina Nelson
Sabrena Stewart
Dave Cofer
Anita Mooney

## Abbreviations

| | |
|---|---|
| AC | Access Control |
| ASSERT | Automated System Security Evaluation and Remediation Tracking |
| AU | Audit and Accountability |
| C&A | Certification and Accreditation |
| CM | Configuration Management |
| EPA | U.S. Environmental Protection Agency |
| FIPS | Federal Information Processing Standards |
| FY | Fiscal Year |
| IV&V | Independent Validation and Verification |
| MA | Maintenance |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| POA&Ms | Plans of Action and Milestones |

U.S. Environmental Protection Agency
Office of Inspector General

10-P-0058
February 2, 2010

# At a Glance

*Catalyst for Improving the Environment*

## Why We Did This Review

We sought to determine whether the U.S. Environmental Protection Agency (EPA) implemented management control processes for maintaining the quality of data in the Automated System Security Evaluation and Remediation Tracking (ASSERT) system.

## Background

EPA uses the ASSERT online tool to gather information regarding testing and evaluating Agency information systems, and tracking progress made in fixing identified security weaknesses. EPA also uses ASSERT to generate reports provided to the Office of Management and Budget pursuant to the Federal Information Security Management Act.

**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/2010/20100202-10-P-0058.pdf**

# *Self-reported Data Unreliable for Assessing EPA's Computer Security Program*

## What We Found

The oversight and monitoring procedures for ASSERT provide limited assurance the data are reliable for assessing EPA's computer security program. As a result:

- Unsubstantiated responses for self-reported information contribute to data quality problems.
- Limited independent reviews and lack of follow-up inhibit EPA's ability to identify and correct data inaccuracies.
- Independent reviews lack coordination with certification and accreditation activities.
- Information security personnel believe they need more training on how to assess security controls and feel pressure to answer system security questions in a positive manner.
- Limited internal reporting on required security controls and missing information in security plans inhibit external reporting.

Further, incomplete security documentation raises concerns as to whether the ASSERT application contractor is meeting federal requirements.

## What We Recommend

We recommend that the Assistant Administrator for Environmental Information issue a memorandum to Assistant Administrators and Regional Administrators emphasizing the importance of ensuring personnel accurately assess and report information in ASSERT.

We also recommend that the Director, Office of Technology Operations and Planning, integrate ongoing independent reviews with the Agency's Certification and Accreditation process, provide periodic training on how to assess and document required minimum security controls, expand the Agency's security reporting process to include collecting information on all required minimum security controls, and implement a process to verify that Agency security plans incorporate all the minimally required system security controls.

The Agency agreed with all of our findings and recommendations.

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

OFFICE OF
INSPECTOR GENERAL

February 2, 2010

**MEMORANDUM**

**SUBJECT:** Self-reported Data Unreliable for Assessing
EPA's Computer Security Program
Report No. 10-P-0058

Rudolph M. Brevard

**FROM:** Rudolph M. Brevard
Director, Information Resources Management Assessments

**TO:** Linda Travers
Acting Assistant Administrator for Environmental Information and
Acting Chief Information Officer

Vaughn Noga
Acting Director, Office of Technology Operations and Planning

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

We sought to determine whether EPA has a mechanism to monitor the quality of self-reported information systems security data. In particular, we assessed to what extent EPA:

- Implemented an organizational structure for monitoring data quality in the Automated System Security Evaluation and Remediation Tracking (ASSERT) system.
- Implemented policies and procedures for managing data quality internally.
- Conducted follow-up activities to ensure responsible officials correct weaknesses.
- Implemented procedures to ensure that the ASSERT contractor adheres to federal information security requirements.

We conducted this audit between January 2008 and September 2009, at EPA Headquarters in Washington, DC, in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

We reviewed information entered in ASSERT as of September 2007. This information represented EPA offices' self-reported compliance status with National Institute of Standards and Technology (NIST) information systems security controls, as part of the Fiscal Year 2007 Federal Information Security Management Act evaluation. Appendix A provides the federal criteria used for this review and a description of ASSERT modules.

We randomly selected 5 NIST security controls and 51 EPA systems in ASSERT that had Fiscal Year 2007 self-reported compliance information. We reviewed the information to determine whether it agreed with the details in the respective systems' security plan. Appendix B contains the list of EPA systems extracted from ASSERT and our methodology and summary of results. Appendix C contains the description of each NIST-reviewed security control.

We surveyed Agency information security personnel who completed the ASSERT Fiscal Year 2007 self-assessments for the reviewed systems. We solicited information on the quality of Agency-provided training and guidance to complete the annual security control self-assessments. We also solicited information as to whether the annual self-assessments added value in helping them protect and evaluate their respective information security programs and whether there was undue pressure by management to answer the self-assessment questions.

The estimated cost of this report – calculated by multiplying the project's staff days by the applicable daily full cost billing rates in effect at the time – is $511,930.

## 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 actions plan for agreed-upon actions, including milestone dates.

We would like to thank your staff for their cooperation. 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 Vincent Campbell, Project Manager, at (202) 566-2540 or campbell.vincent@epa.gov.

# Self-reported Data Unreliable for Assessing EPA's Computer Security Program

Results of Review

# Audit Methodology

- Reviewed self-reported system security information entered in the Automated System Security Evaluation and Remediation Tracking (ASSERT) system as of September 2007.

- Reviewed EPA's organizational structure responsible for managing the quality of data in the ASSERT system.

- Evaluated self-reported system security information for 51 EPA systems. Reviewed information for compliance with five required National Institute of Standards and Technology (NIST) security controls.

- Surveyed Agency information security personnel who entered the self-reported system security information into ASSERT. Solicited opinions on the quality of training, guidance, and management support for self-reporting system security information.

- Evaluated EPA procedures used to ensure the ASSERT contractor adheres to federal system security guidance.

# Noted Accomplishments

In response to Office of Inspector General audit, *EPA's Computer Security Self-Assessment Needs Improvement*, Report No. 2003-P-00017, September 30, 2003, Office of Environmental Information:

- Updated the ASSERT application to include a test and an implement control feature.
- Developed and implemented an independent verification and validation process to monitor and evaluate self-assessment responses in ASSERT.
- Developed and implemented technical vulnerability assessment lab methodology to evaluate authentication and identification controls.
- Issued an Agency-wide memorandum stipulating all security plans must be prepared in compliance with NIST.

# Finding 1

## Better Data Quality Processes Needed to Improve Accuracy of Self-reported Data

# Better Data Quality Processes Needed to Improve Accuracy of Self-reported Data

## Unsubstantiated Responses for Self-reported System Security Information Contribute to Data Quality Problems

- Only 17% (71 of 408) of self-reported ASSERT entries had supporting information in security plans.

- Unsubstantiated responses resulted from EPA offices:
  - Entering ASSERT data based on institutional knowledge rather than information documented in the security plan.
  - Preparing the security plans in a general manner that did not include specific details on how each security control is implemented.
  - Using risk assessment results that did not fully test NIST security controls.

# Better Data Quality Processes Needed to Improve Accuracy of Self-reported Data

## Limited Independent Validation & Verification (IV&V) and Lack of Follow-up Inhibit EPA's Ability to Identify and Correct Data Inaccuracies

- From Fiscal Year (FY) 2005 through 2007, 15 IV&V assessments were conducted - *(9% of the 171 systems tracked in ASSERT).*

- No requirement for EPA offices to enter Plans of Action and Milestones (POA&Ms) in ASSERT for unresolved IV&V findings.

- EPA offices not required to provide documentation to EPA's Technology and Information Security Staff to support steps taken to resolve findings.

# Better Data Quality Processes Needed to Improve Accuracy of Self-reported Data

## IV&V Program Lacks Coordination With Certification & Accreditation (C&A) Activities

- IV&V Process:
  - Takes place after EPA offices complete security activities associated with authorizing their system for operation.
  - Does not focus on whether EPA offices designed planned security activities according to applicable guidance and executed the plans as planned.
  - Lacks method to assist system owners in designing and executing C&A activities consistent with federal guidance.
  - Does not identify and track identified weaknesses along with corrective actions.

# OIG Recommendation

Director, Office of Technology Operations and Planning should:

1-1 Develop and implement an assessment process that integrates independent reviews with the Agency's Certification and Accreditation process. The newly structured assessment process should focus more on ensuring EPA offices (a) plan and execute security activities required to authorize system operations, and (b) complete security activities that comply with federal and Agency guidance. The newly structured process should also ensure EPA offices create Plans of Action and Milestones for any identified weaknesses. The newly structured process should also track identified weaknesses and ensure EPA offices retain documentation that supports the remediation of all identified weaknesses.

# EPA's Response to Briefing

EPA indicated it would perform the following actions:

- Implement a quality review process along with establishing an interagency agreement to improve the quality of the C&A products and reporting of POA&Ms.
- Hire an information security person to manage POA&Ms based on results from internal and external reviews.
- Adopt a manual escalation procedure to the Senior Information Official to remediate unresolved POA&Ms. This process is expected to be automated using a new C&A tool (Telos Xacta). The automated process will help eliminate arbitrary date shifts and permit storage of C&A artifacts. ASSERT will be modified to facilitate these activities.
- Increase the IV&V review to cover 10% of the Agency's information systems along with full coverage of all financial systems and the associated general support systems.

# Finding 2

**Better Guidance and Management Support Needed to Foster Accurate Security Reporting**

# Better Guidance and Management Support Needed to Foster Accurate Security Reporting

## Not Properly Assessing Security Controls Contributes to Invalid Data in ASSERT

Survey responses regarding the level of training, guidance, and management support for self-reporting system security information disclosed:

- 68% of respondents believed they had not been educated on how to fully assess the NIST 800-53 security controls in ASSERT. Some respondents are confused about how to assess controls when there are shared responsibilities between the general support system and major applications, or between Headquarters and regional offices. Respondents stated that Agency personnel typically refer them to NIST policies for guidance, instead of providing direct assistance when there is uncertainty about how to assess a security control within the ASSERT application.

# Better Guidance and Management Support Needed to Foster Accurate Security Reporting

## Not Properly Assessing Security Controls Contributes to Invalid Data in ASSERT *(Continued)*

- 47% of respondents believed more training is needed when EPA introduces newer versions of ASSERT.  Respondents indicated that ASSERT has gone through numerous changes and updates that have contributed to a longer learning curve.  Respondents believe EPA could have done a better job in communicating system changes, providing notice when training would be given, and scheduling training in advance of critical ASSERT due dates.

- 68% of respondents felt pressured to answer system security questions in ASSERT in a positive way, even in situations where a specific security control had not been properly tested and implemented.  Some respondents believe that the emphasis is on EPA maintaining an “A” rating on the federal information security scorecard.  Some respondents felt the lack of resources and time constraints led them to view providing self-reported system security information as a “check-the-box” exercise, with the emphasis on using the ASSERT application instead of assessing security.

# OIG Recommendations

Director, Office of Technology Operations and Planning should:

2-1 Provide periodic training (at least quarterly and during the annual Security Conference) on how to assess and document the implementation of minimum security controls as required by NIST guidance.

Assistant Administrator for Environmental Information and Chief Information Officer should:

2-2 Issue a memorandum to Assistant and Regional Administrators to emphasize the importance of ensuring personnel accurately assess and report security information in the ASSERT system.

# EPA's Response to Briefing

EPA indicated it would take the following actions:

- Implement quarterly training sessions on the C&A activities.
- Implement a 3-day hands-on "road show" with Agency system staff to review specific information security packages and associated POA&Ms.
- Implement a mandatory review of all draft and new NIST documents via Quick Place and discuss how the documents apply to EPA.
- Negotiate a baseline and refresher role-based training course as part of the Agency's Information Security Training, Education and Awareness curriculum for C&A.
- Prepare a memorandum from the Chief Information Officer on the importance of accurately assessing and reporting security information in the ASSERT system.

# Finding 3

EPA Not Fully Reporting the Status of Its Security Program

# EPA Not Fully Reporting the Status of Its Security Program

## Limited Internal Reporting on Required Information System Security Controls Inhibits External Reporting

- EPA offices evaluated and provided self-reported information on only 24% (41 of 171) of the required NIST controls as part of the Agency's annual review of its information security program.

- Evaluation excluded all security controls associated with the (1) Media Protection, and (2) System and Communications Protection security categories.

# EPA Not Fully Reporting the Status of Its Security Program

## Missing Information in Security Plans Fosters Incomplete Reporting on EPA's Security Program

- EPA offices lacked the information needed to answer system security questions.
  - EPA offices lacked up-to-date security plans. 80% of reviewed security plans had not been updated since NIST issued the first revision of Special Publication 800-53, *Recommended Security Controls for Federal Information Systems,* in December 2006.
  - Only 2 of the 10 reviewed security plans documented all the NIST security controls.

# OIG Recommendations

Director, Office of Technology Operations and Planning should:

3-1 Expand the Agency's annual system security self-reporting process to include collecting information on all NIST minimum required system security controls.

3-2 Implement a process to verify that Agency security plans incorporate all the minimum required system security controls as prescribed by NIST. This process should include establishing a target date by which the Agency security plans will comply with the current NIST guidance.

# EPA's Response to Briefing

EPA indicated it would take the following actions:

- Procure a new C&A Tool (Telos Xacta). Once implemented, the tool will require all C&A artifacts to be published, stored and maintained.
- Implement a quality review process for C&A activities and newly published NIST documents.
- Develop an Agency governance board to ensure newly issued federal requirements are implemented in a timely fashion.

# Finding 4

ASSERT Application Needs Security Planning

# ASSERT Application Needs Security Planning

## Incomplete Security Documentation Raises Concerns Whether the ASSERT Application Contractor is Meeting Federal Requirements

- ASSERT application security plan does not comply with federal security requirements. The security plan lacks specific information on how the required NIST security controls were implemented for three of the five reviewed areas.

- ASSERT application lacks an approved contingency plan.

# EPA's Response to Briefing

Based on our audit, EPA took the following actions:

- Updated the ASSERT C&A packages in accordance with applicable NIST guidance.

- Updated and approved the ASSERT Contingency Plan in accordance with applicable NIST guidance.

# *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 |
| 1-1 | 8 | Develop and implement an assessment process that integrates independent reviews with the Agency's Certification and Accreditation process. The newly structured assessment process should focus more on ensuring EPA offices (a) plan and execute security activities required to authorize system operations, and (b) complete security activities that comply with federal and Agency guidance. The newly structured process should also ensure EPA offices create Plans of Action and Milestones for any identified weaknesses. The newly structured process should also track identified weaknesses and ensure EPA offices retain documentation that supports the remediation of all identified weaknesses. | O | Director, Office of Technology Operations and Planning | | | |
| 2-1 | 13 | Provide periodic training (at least quarterly and during the annual Security Conference) on how to assess and document the implementation of minimum security controls as required by NIST guidance. | O | Director, Office of Technology Operations and Planning | | | |
| 2-2 | 13 | Issue a memorandum to Assistant and Regional Administrators to emphasize the importance of ensuring personnel accurately assess and report security information in the ASSERT system. | O | Assistant Administrator for Environmental Information and Chief Information Officer | | | |
| 3-1 | 18 | Expand the Agency's annual system security self-reporting process to include collecting information on all NIST minimum required system security controls. | O | Director, Office of Technology Operations and Planning | | | |
| 3-2 | 18 | Implement a process to verify that Agency security plans incorporate all the minimum required system security controls as prescribed by NIST. This process should include establishing a target date by which the Agency security plans will comply with the current NIST guidance. | O | Director, Office of Technology Operations and Planning | | | |

[1] 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**

# *Audit Criteria and Description of ASSERT Modules*

## Applicable Federal Guidance

- Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal Government.
- NIST 800-18, *Guide for Developing Security Plans for Information Systems,* states that system security plans should provide a thorough description of how minimum security controls are being implemented or planned to be implemented.
- NIST 800-34, *Contingency Planning Guide for Information Technology Systems,* provides instructions, recommendations, and considerations for Information Technology Systems contingency planning. Contingency planning contains interim measures to recover IT services following an emergency or system disruption.
- NIST 800-53, *Recommended Security Controls for Federal Information Systems,* provides guidance to federal agencies implementing FIPS 200. The 17 security control families in NIST 800-53 are closely aligned with the 17 security-related areas in FIPS 200 for protecting federal information.

## Description of ASSERT System Modules

ASSERT contains three modules: (1) Security Self-Assessments, (2) Remediation Tracking, and (3) System Categorization.

The ASSERT system security self-assessment module is based on NIST 800-53. The electronic entry of the responses to the assessment and EPA-established goals will automatically create POA&Ms to remediate vulnerabilities identified in the assessment.

The ASSERT remediation module electronically creates an EPA-established standardized approach for developing POA&Ms that respond to weaknesses developed by assessment or security reviews. POA&M tasks can be automatically generated by the self-assessment process or entered manually for tasks generated by other sources.

ASSERT systems are categorized based on the system's needed level of confidentiality, integrity, and availability, as explained in FIPS 199 guidelines.

**Appendix B**

# *OIG Analysis of Results*

We selected the following five system-specific security controls to determine whether the system's security plans fully supported the self-assessments, as reported in EPA's ASSERT.

| Technical Controls | | Operational Controls | |
|---|---|---|---|
| (AC-2) | Account Management | (CM-5) | Configuration Management: Access Restriction for Change |
| (AC-13) | Supervision and Review | (MA-2) | Maintenance: Controlled Maintenance |
| (AU-2) | Auditable Events | | |

**Source: OIG compiled data based on security controls selected from NIST Special Publication 800-53.**

Appendix C contains the description of the security controls and the associated enhancements reviewed.

We reviewed 408 data entries associated with these security controls. Only 17 percent (71 of 408) of the ASSERT data entries were supported by systems security plans.

## Assessment Methodology

The security controls we reviewed were unique to the 51 systems listed in the following table. Each security control evaluated had to receive a passing grade of "Yes" in order for the comparative analysis between the ASSERT data and security plan to receive a cumulative passing grade. Any security control that received a nonpassing grade of "No" would result in a cumulative nonpassing grade. We did not project any errors to EPA's universe of systems in ASSERT, because our sample was not statistically selected.

The base control and enhancements are indicated in the following table by the following abbreviations:

BC - Base control
E1 - Enhancement 1
E2 - Enhancement 2
E3 - Enhancement 3
E4 - Enhancement 4

The information below identifies the 51 systems selected from ASSERT as part of this audit and the results of our analysis.

| | | | **Did the system security plan support the FY2007 self-assessment in EPA's ASSERT database?** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **System Category** | **System Name** | **Program or Regional Office** | **AC-2** | | | | | **AC-13** | | **AU-2** | **CM-5** | | **MA-2** | | |
| | | | **BC** | **E1** | **E2** | **E3** | **E4** | **BC** | **E1** | **BC** | **BC** | **E1** | **BC** | **E1** | **E2** |
| | | | | | | | | | | | | | | | |
| **High** | NAREL Radiation Network | Office of Air and Radiation | N | N | N | N | N | N | N | N | N | N | N | N | N |
| **Moderate** | EEONet | Office of the Administrator | N | N | N | N | - | N | - | N | N | - | N | N | - |
| | Energy Star | Office of Air and Radiation | Y | Y | Y | N | - | Y | - | N | Y | - | Y | Y | - |
| | LNS | Office of Air and Radiation | N | N | N | N | - | N | - | N | N | - | N | N | - |
| | OAR LAN- 1310 | Office of Air and Radiation | N | N | N | N | - | N | - | N | N | - | N | N | - |
| | Federal Retirement Benefits Calculator | Office of Administration and Resources Management | N | N | N | N | - | N | - | N | N | - | N | N | - |
| | Grants Information Control System | Office of Administration and Resources Management | N | N | N | N | - | N | - | N | N | - | N | N | - |
| | Budget Automation System | Office of Chief Financial Officer | N | Y | N | Y | - | N | - | N | N | - | N | N | - |
| | Contract Payment System | Office of Chief Financial Officer | N | N | N | N | - | N | - | Y | N | - | Y | Y | - |
| | Financial Data Warehouse | Office of Chief Financial Officer | N | N | N | N | - | N | - | N | N | - | N | N | - |
| | PeoplePlus | Office of Chief Financial Officer | Y | N | Y | N | - | Y | - | Y | Y | - | N | N | - |
| | NEIC LAN | Office of Enforcement Compliance and Assurance | Y | Y | Y | N | - | Y | - | Y | Y | - | N | N | - |
| | OECA LAN | Office of Enforcement Compliance and Assurance | N | N | N | N | - | N | - | N | N | - | N | N | - |

|  |  |  | Did the system security plan support the FY2007 self-assessment in EPA's ASSERT database? |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| System Category | System Name | Program or Regional Office | AC-2 |  |  |  |  | AC-13 |  | AU-2 | CM-5 |  | MA-2 |  |  |
|  |  |  | BC | E1 | E2 | E3 | E4 | BC | E1 | BC | BC | E1 | BC | E1 | E2 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Waste International Tracking System | Office of Enforcement Compliance and Assurance | N | Y | N | N | - | Y | - | N | N | - | N | N | - |
|  | AAA Remote Access System | Office of Environmental Information | N | N | N | N | - | N | - | N | N | - | N | N | - |
|  | Active Directory | Office of Environmental Information | N | N | N | N | - | N | - | N | N | - | N | N | - |
|  | Automated System Security Evaluation and Remediation Tracking | Office of Environmental Information | Y | N | Y | Y | - | N | - | Y | Y | - | N | N | - |
|  | Enterprise Server | Office of Environmental Information | N | N | N | N | - | N | - | N | Y | - | N | N | - |
|  | EPA Enterprise Portal | Office of Environmental Information | N | N | N | N | - | N | - | N | N | - | N | N | - |
|  | Internet Operations and Maintenance and Enhancements | Office of Environmental Information | N | N | N | N | - | N | - | N | N | - | N | N | - |
|  | Remedy | Office of Environmental Information | N | N | N | N | - | N | - | N | Y | - | N | N | - |
|  | SRA Arlington | Office of Environmental Information | Y | Y | Y | Y | - | Y | - | Y | Y | - | Y | Y | - |
|  | Shared Services | Office of Environmental Information | N | N | N | N | - | N | - | N | N | - | N | N | - |
|  | WebForms | Office of Environmental Information | N | N | N | N | - | N | - | N | N | - | N | N | - |
|  | OGC Local Area Network | Office of General Counsel | N | N | N | Y | - | N | - | N | N | - | N | N | - |
|  | Office of Pesticide Programs Information Network | Office of Prevention, Pesticides and Toxic Substances | N | Y | N | N | - | N | - | N | N | - | N | N | - |
|  | OPP LAN | Office of Prevention, Pesticides and Toxic Substances | N | N | N | N | - | N | - | Y | N | - | N | N | - |

| | | | Did the system security plan support the FY2007 self-assessment in EPA's ASSERT database? | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **System Category** | **System Name** | **Program or Regional Office** | **AC-2** | | | | | **AC-13** | | **AU-2** | **CM-5** | | **MA-2** | | |
| | | | **BC** | **E1** | **E2** | **E3** | **E4** | **BC** | **E1** | **BC** | **BC** | **E1** | **BC** | **E1** | **E2** |
| | | | | | | | | | | | | | | | |
| | OPPT Admin LAN | Office of Prevention, Pesticides and Toxic Substances | **N** | **N** | **N** | **N** | - | **N** | - | **N** | **N** | - | **N** | **N** | - |
| | OPPT CBI LAN | Office of Prevention, Pesticides and Toxic Substances | **N** | **N** | **N** | **N** | - | **N** | - | **N** | **N** | - | **N** | **N** | - |
| | Office of Research and Development Management Info | Office of Research and Development | **N** | **N** | **N** | **N** | - | **N** | - | **N** | **N** | - | **N** | **N** | - |
| | Office of Research and Development RTP GSS | Office of Research and Development | **N** | **N** | **N** | **N** | - | **N** | - | **N** | **N** | - | **N** | **N** | - |
| | SRMP | Office of Solid Waste and Emergency Response | **N** | **N** | **N** | **N** | - | **N** | - | **N** | **N** | - | **N** | **N** | - |
| | OGWDW LAN Container | Office of Water | **N** | **N** | **N** | **N** | - | **N** | - | **N** | **N** | - | **N** | **N** | - |
| | OWOW LAN Container | Office of Water | **Y** | **Y** | **Y** | **Y** | - | **Y** | - | **Y** | **Y** | - | **N** | **Y** | - |
| | STORET | Office of Water | **N** | **Y** | **Y** | **Y** | - | **N** | - | **N** | **N** | - | **N** | **N** | - |
| | Region 2 LAN | Region 2 | **Y** | **N** | **N** | **N** | - | **N** | - | **Y** | **N** | - | **N** | **N** | - |
| | Region 4 LAN | Region 4 | **N** | **N** | **N** | **N** | - | **N** | - | **Y** | **N** | - | **N** | **N** | - |
| | GSSP for R5 USEPA | Region 5 | **N** | **N** | **N** | **N** | - | **N** | - | **N** | **N** | - | **N** | **N** | - |
| | Region 7 LAN | Region 7 | **N** | **N** | **N** | **N** | - | **N** | - | **N** | **Y** | - | **N** | **N** | - |
| | Region 8 LAN | Region 8 | **N** | **N** | **N** | **N** | - | **N** | - | **N** | **N** | - | **N** | **N** | - |
| **Low** | OTAQ-IO NDS Container-ARB | Office of Air and Radiation | **N** | - | - | - | - | **N** | - | **N** | N/A | - | **N** | - | - |
| | FIFRA/TSCA Tracking Systems National Compliance Database | Office of Enforcement Compliance and Assurance | **Y** | - | - | - | - | **N** | - | **N** | N/A | - | **Y** | - | - |
| | Laboratory Inspection and Study Audit | Office of Enforcement Compliance and Assurance | **N** | - | - | - | - | **N** | - | **N** | N/A | - | **N** | - | - |
| | Architecture Repository and Tool | Office of Environmental Information | **Y** | - | - | - | - | **N** | - | **Y** | N/A | - | **Y** | - | - |

| | | | **Did the system security plan support the FY2007 self-assessment in EPA's ASSERT database?** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **System Category** | **System Name** | **Program or Regional Office** | **AC-2** | | | | | **AC-13** | | **AU-2** | **CM-5** | | **MA-2** | | |
| | | | **BC** | **E1** | **E2** | **E3** | **E4** | **BC** | **E1** | **BC** | **BC** | **E1** | **BC** | **E1** | **E2** |
| | | | | | | | | | | | | | | | |
| | Toxic Release Inventory-Made Easy | Office of Environmental Information | N | - | - | - | - | N | - | N | N/A | - | N | - | - |
| | Voice over IP | Office of Environmental Information | Y | - | - | - | - | Y | - | N | N/A | - | Y | - | - |
| | National Homeland Security Research Center - CINC | Office of Research and Development | N | - | - | - | - | N | - | N | N/A | - | N | - | - |
| | Nheerl-Corvallis | Office of Research and Development | N | - | - | - | - | N | - | Y | N/A | - | Y | - | - |
| | Nheerl-Gulf Breeze | Office of Research and Development | N | - | - | - | - | N | - | N | N/A | - | N | - | - |
| | Assessment, Cleanup & Redevelopment Exchange System | Office of Solid Waste and Emergency Response | N | - | - | - | - | N | - | Y | N/A | - | N | - | - |
| | Institutional Controls Tracking System | Office of Solid Waste and Emergency Response | N | - | - | - | - | N | - | Y | N/A | - | N | - | - |
| **Total Number of Entries = 408** | | | **51** | **40** | **40** | **40** | **1** | **51** | **1** | **51** | **40** | **1** | **51** | **40** | **1** |
| **(Total Number of Supportable Entries (denoted with Y) = 71** | | | **10** | **8** | **7** | **6** | **0** | **7** | **0** | **13** | **9** | **0** | **7** | **4** | **0** |

**Y = Yes**

**N = No**

**Dash (-) means the enhancement was not a required security control to be evaluated based on the application's system category.**

**N/A = Per NIST Special Publication 800-53 Rev. 1, *Recommended Security Controls for Federal Information Systems*, December 2006, configuration management (CM-5) access restriction for change is not a required security control to be assessed for "low-impact" information systems. Additionally, this security control was not listed as an evaluation control in ASSERT for Agency systems reviewed with a "low" system categorization. Therefore, the OIG did not believe it was necessary to conduct audit work on this security control.**

**Source: OIG-compiled data based on EPA's ASSERT data and security plans**.

**Appendix C**

# *Description of Reviewed Security Controls*

The information below provides the description of each base control and the associated control enhancements for the applicable system risk categorization. The source for this table is NIST Special Publication 800-53 Rev. 1, *Recommended Security Controls for Federal Information Systems*, December 2006.

| **System Risk Categorization** | | | |
|---|---|---|---|
| ***Class: Technical*** | ***High*** | ***Moderate*** | ***Low*** |
| **Security Control Family: Access Control (AC)** | | | |
| **AC-2 Account Management**:<br>**Base Control**: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts. | X | X | X |
| **Control Enhancements:**<br>(1) The organization employs automated mechanisms to support the management of information system accounts. | X | X | |
| (2) The information system automatically terminates temporary and emergency accounts [Assignment: organization-defined time period for each type of account]. | X | X | |
| (3) The information system automatically disables inactive accounts after [Assignment: organization-defined time period]. | X | X | |
| (4) The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals. | X | X | |

| System Risk Categorization | | | |
|---|---|---|---|
| ***Class: Technical*** | ***High*** | ***Moderate*** | ***Low*** |
| **Security Control Family: Access Control (AC)** | | | |
| **AC-13 Supervision and Review - Access Control**<br>**Base Control**: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. | X | X | X |
| **Control Enhancement:** The organization employs automated mechanisms to facilitate the review of user activities. | X | X | |
| **Security Control Family: Audit and Accountability (AU)** | | | |
| **AU-2 Auditable Events**<br>**Base Control**: The information system generates audit records for the following events: [Assignment: organization-defined auditable events]. | X | X | X |
| **Control Enhancements**:<br>(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail. | X | | |
| (2) The information system provides the capability to manage the selection of events to be audited by individual components of the system. | X | | |
| (3) The organization periodically reviews and updates the list of organization-defined auditable events. | X | X | |

| **System Risk Categorization** | | | |
|---|---|---|---|
| ***Class: Operational*** | ***High*** | ***Moderate*** | ***Low*** |
| **Security Control Family: Configuration Management (CM)** | | | |
| **CM-5 Access Restriction for Change**<br>**Base Control**: The organization approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system, and generates, retains, and reviews records reflecting all such changes. | X | X | N/A |
| **Control Enhancement:** The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions. | X | | |
| **Security Control Family: Maintenance (MA)** | | | |
| **MA-2 Controlled Maintenance**<br>**Base Control:** The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. | X | X | X |
| **MA-2 Controlled Maintenance**<br>**Control Enhancements:**<br>(1) The organization maintains maintenance records for the information system that include: (a) the date and time of maintenance; (b) name of the individual performing the maintenance; (c) name of escort, if necessary; (d) a description of the maintenance performed; and (e) a list of equipment removed or replaced (including identification numbers, if applicable).<br>(2) The organization employs automated mechanisms to schedule and conduct maintenance as required, and to create up-to-date, accurate, complete, and available records of all maintenance actions, both needed and completed. | X<br>X | X<br>X | |

Appendix D

# *Distribution*

Office of the Administrator
Acting Assistant Administrator for Environmental Information and Chief Financial Officer
Acting Director, Office of Technology Operations and Planning,
Office of Environmental Information
Acting Director, Technology and Information Security Staff,
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
Audit Follow-up Coordinator, Office of Environmental Information
Acting Inspector General