U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Briefing Report

Steps Taken But More Work Needed to Strengthen Governance, Increase Utilization, and Improve Security Planning for the Exchange Network

Report No. 09-P-0184

June 30, 2009

Report Contributors

Rudolph M. Brevard
Cheryl Reid
David Cofer
Anita Mooney
Sejal Shah
Christina Nelson

Abbreviations

ASSERT	Automated System Security Evaluation and Remediation Tracking
CDX	Central Data Exchange
EPA	U.S. Environmental Protection Agency
NIST	National Institute for Standards and Technology
OIG	Office of Inspector General
SP	Special Publication

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

OFFICE OF
INSPECTOR GENERAL

June 30, 2009

MEMORANDUM

SUBJECT: Steps Taken But More Work Needed to Strengthen Governance, Increase Utilization, and Improve Security Planning for the Exchange Network
Report No. 09-P-0184

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

TO: Linda Travers
Acting Assistant Administrator and Chief Information Officer
Office of Environmental Information

Lisa Schlosser
Director, Office of Information Collection
Office of Environmental Information

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 consists of the briefing presentation we provided to Office of Environmental Information managers on May 4, 2009. 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 taken:

- Corrective actions for recommendations made in the audit report *Improved Management Practices Needed to Increase Use of Exchange Network*, Report No. 2007-P-00030 issued August 20, 2007; and
- Steps to ensure all Exchange Network components comply with federal security requirements.

We conducted this audit from January through May 2009 at EPA Headquarters in Washington, DC, in accordance with the 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 interviewed EPA personnel responsible for implementing the corrective actions in the prior report and personnel responsible for managing the security activities reviewed. We reviewed relevant security documents and evaluated them against prescribed federal and EPA guidance. We reviewed self-reported security information entered into the Agency's Automated System Security Evaluation and Remediation Tracking (ASSERT) system and compared it against information contained in the provided security documents.

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 $253,562.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report. We are requesting your response within 45 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 Cheryl Reid, Project Manager, at (919) 541-2256 or reid.cheryl@epa.gov.

Steps Taken But More Work Needed to Strengthen Governance, Increase Utilization, and Improve Security Planning for the Exchange Network

Results of Review

Objective 1

Status of Prior Audit Report Recommendations

Prior Audit Report Recommendations

- **Recommendation 2.1 -** Acting Assistant Administrator for Environmental Information execute recently developed Exchange Network Communications and Marketing Plan elements that include actively promoting the business value of participating in Network initiatives to EPA and partner environmental program managers.

  Status - Ongoing and progressing

Prior Audit Report Recommendations (Cont.)

- **Recommendation 2.2** - Acting Assistant Administrator for Environmental Information modify Exchange Network change management policies and procedures to include step-by-step processes for fully testing and certifying all implementation tools before release to the Exchange Network community.

  Status – Completed; published *Principles, Rules, and Procedures for Change Management on the Exchange Network*, V1.1, February 19, 2009.

Prior Audit Report Recommendations (Cont.)

- **Recommendation 3.1** - Acting Assistant Administrator for Environmental Information work with Exchange Network governance bodies to develop and implement a process that uses the Network Business plan criteria to evaluate data flows for future Network implementation.

  Status – Completed; published *2009 Annual Exchange Network Grant Program Solicitation Notice,* September, 2008.

Prior Audit Report Recommendations (Cont.)

- **Recommendation 4.1** - Acting Assistant Administrator for Environmental Information develop a new milestone plan for completing the Exchange Network performance measures project.

  Status – Completed; first Performance Measures reported May 2008.

Prior Audit Report Recommendations (Cont.)

- **Recommendation 4.2** - Acting Assistant Administrator for Environmental Information develop procedures for establishing ad-hoc workgroups for Exchange Network projects.

  Status - Unimplemented

Prior Audit Report Recommendations (Cont.)

- **Recommendation 5.1** - Acting Assistant Administrator for Environmental Information publish standards that specify when EPA program offices must use the Exchange Network when modernizing or developing applications. The standards should also specify the processes EPA offices must follow when the office cannot adhere to the established standards or select an alternate technology solution to the one prescribed.

  Status - Unimplemented

Prior Audit Report Recommendations (Cont.)

- **Recommendation 5.2** - Acting Assistant Administrator for Environmental Information include the Exchange Network and related technologies as part of the Agency's Enterprise Architecture.

  Status - Unimplemented

Prior Audit Report Recommendations (Cont.)

- **Recommendation 5.3** - Acting Assistant Administrator for Environmental Information have Office of Information Collection complete its plans to develop a tool offices can use to evaluate their applications in regard to Network technologies.

  Status – Completed March 27, 2008; created a Return on Investment Estimator tool for program offices to use in the early stages of planning new data flows.

OIG Recommendations

The Acting Assistant Administrator for Environmental Information should:

1. Submit an updated Corrective Action Plan for unimplemented recommendations 4-2, 5-1, and 5-2.

2. Update EPA's Management Audit Tracking System regarding unimplemented recommendations.

Objective 2

Compliance with Federal Security Requirements

Certification & Accreditation (C&A)

- The current Central Data Exchange (CDX) Certification and Accreditation package is not in compliance with federal security requirements because the approved system security plan, the security assessment report, and the plan of action and milestones do not meet federal and agency requirements.

Security Plan & Risk Assessment

- Minimum Security Controls are not in compliance with latest National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 1.
- Security plan does not comply with NIST SP 800-18, Revision 1, because the Minimum Security Controls Section does not thoroughly describe how each security control is being implemented, or planned to be implemented.
- The latest CDX Risk Assessment, dated December 22, 2004, is outdated.

Contingency Plan

- Record of Changes is not maintained, as required by NIST SP 800-34 guidance and the EPA's Agency Network Security Policy.

- Office of Environmental Information did not provide documentation to (1) support the existence of a training plan that meets federal policy or guidance, and (2) confirm personnel have been trained on contingency plan responsibilities and procedures within the last two years.

- Office of Environmental Information has not conducted annual Contingency Plan testing, as required by the CDX Contingency Plan, Section 5. Last test was conducted in March 2006.

ASSERT Reporting

- ASSERT reporting for CDX is not accurate.

  Only:

  - 33% of the ASSERT data reviewed is supported by the corresponding data in the official security plan.
  - 25% of the ASSERT assessment entries are compliant with NIST SP 800-18, Revision 1.
  - 42% of the control elements evaluated in the official security plan are compliant with NIST SP 800-18, Revision 1.

Vulnerability Scanning

- Monthly server full system scans and Patchlink reports are not performed, as required by both EPA and CDX policy and procedures.

- Weekly server full system scans are not being performed, as required by both EPA and CDX policy and procedures.

Summary

- Steps needed to ensure the Exchange Network is fully recognized as the preferred method for exchanging environmental information between EPA and its partners, and to strengthen Exchange Network governance.
- Emphasis needed to ensure CDX meets the prescribed federal security requirements.

Without action, management hinders its ability to achieve the desired utilization of the Exchange Network and ensure the Network is operating without vulnerabilities that could put needed data at risk.

OIG Recommendations

The Director, Office of Information Collection should:

3. Recertify and reaccredit CDX.

4. Update the CDX Security Plan to comply with NIST SP 800-18, and ensure the plan describes how CDX implements the minimum security controls contained in NIST SP 800-53.

5. Conduct a formal, independent risk assessment of CDX; and ensure CDX is reassessed every three years, as required by EPA policy.

OIG Recommendations (cont.)

6. Maintain the CDX Contingency Plan Record of Changes, as required by NIST SP 800-34 guidance and EPA's Network Security Policy.

7. Develop a CDX Contingency Plan training plan that meets federal requirements and ensure personnel with contingency plan responsibilities receive required training on responsibilities and procedures.

8. Conduct CDX Contingency Plan testing at least annually, as required by Agency policy and NIST guidance.

OIG Recommendations (cont.)

9. Ensure data entered into ASSERT are supported either by the system security plan or by other documents referenced in the system security plan.

10. Perform required weekly and monthly network vulnerability testing, as required by EPA and CDX policy and procedures.

11. Issue an Interim Authorization to Operate CDX until CDX is reaccredited.

12. Enter a Plan of Actions and Milestones in the Agency's information security weakness tracking system for recommendations 3 through 11.