U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Information Technology

EPA Needs to Improve Security Planning and Remediation of Identified Weaknesses in Systems Used to Protect Human Health and the Environment

Report No. 16-P-0006 **October 14, 2015**

Report Contributors:

Rudolph M. Brevard
Albert Schmidt
Sabrena Stewart
Gina Ross
Vincent Campbell
Jeremy Sigel

Abbreviations

ASSERT	Automated System Security Evaluation and Remediation Tracking
ATO	Authorization to Operate
CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Management Act of 2002
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OIG	Office of Inspector General
POA&M	Plan of Action and Milestones
SAISO	Senior Agency Information Security Officer

U.S. Environmental Protection Agency
Office of Inspector General

16-P-0006
October 14, 2015

At a Glance

Why We Did This Audit

The U.S. Environmental Protection Agency (EPA), Office of Inspector General, sought to determine whether the EPA implemented management control processes for maintaining the quality of data in Xacta.

Xacta is the EPA's official system for recording and maintaining information about the agency's compliance with mandated information system security requirements. Protecting this system and its data is important because it (1) allows EPA executives to make risk-based decisions regarding the continued operations of the EPA's information technology resources and (2) serves as a source for external reporting on the EPA's compliance with the Federal Information Security Management Act.

This report addresses the following EPA goal or cross-agency strategy:

- *Embracing EPA as a high-performing organization.*

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

The full report is at:
www.epa.gov/oig/reports/2016/20151014-16-P-0006.pdf

EPA Needs to Improve Security Planning and Remediation of Identified Weaknesses in Systems Used to Protect Human Health and the Environment

What We Found

The EPA uses Xacta to track offices' compliance with mandated federal information system requirements and management of identified information system weaknesses. Prior to implementing Xacta, the EPA used Automated Systems Security Evaluation and Remediation Tracking for similar purposes and we previously reported that the EPA needed to improve internal controls regarding the quality of the data it uses for decision making.

EPA's network security is essential to provide the information, technology and services necessary to advance the protection of human health and the environment.

While the EPA indicated it took steps to improve the completeness and accuracy of reported information system security data, more management emphasis is needed to ensure that Xacta is authorized to operate in accordance with federally mandated requirements and that offices manage known system weaknesses. In particular, Xacta was placed into service without complete and properly approved information system documentation. Additionally, EPA security personnel are not developing a required Plan of Action and Milestones in a timely manner to manage the remediation of known vulnerabilities as required by agency guidance. As a result, the EPA cannot be assured that Xacta provides the protection necessary to safeguard key information security data needed for decision-making and external reporting. Furthermore, known vulnerabilities continue to place the EPA's network at risk to be exploited because management lacks information to implement remediation activities.

Recommendations and Planned Corrective Actions

We recommend that the Chief Information Officer undertake a number of corrective actions to address security planning in the EPA's risk management system and improve processes for remediating known weaknesses. These corrective actions include development of information system documentation for Xacta to comply with established guidance; complete reauthorization of Xacta; conduct a review of the EPA's process to reauthorize information systems; implement a process for using Xacta to manage vulnerabilities; and implement Xacta support to simplify most users' tasks within the system.

The agency took steps to complete corrective actions on four of the five recommendations. After subsequent meetings with the agency, we agreed to revise the fifth recommendation to clarify our concerns. The agency agreed with this revised recommendation and provided a planned date when it would complete the planned corrective action. This recommendation is considered open with agreed-to corrective action pending.

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

THE INSPECTOR GENERAL

October 14, 2015

MEMORANDUM

SUBJECT: EPA Needs to Improve Security Planning and Remediation of Identified Weaknesses in Systems Used to Protect Human Health and the Environment
Report No. 16-P-0006

FROM: Arthur A. Elkins Jr.

TO: Ann Dunkin, Chief Information Officer
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 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.

The office we identified with primary jurisdiction over the audit issues and the responsibility for taking corrective action on our recommendations is the Office of Environmental Information.

Action Required

You are not required to provide a written response to this final report because you provided agreed-to corrective actions and planned completion dates for the report recommendations. The OIG may make periodic inquiries on your progress in implementing these corrective actions. Please update the EPA's Management Audit Tracking System as you complete planned corrective actions. Should you choose to provide a final response, we will post your response on the OIG's public website, along with our memorandum commenting on your response. You should provide your response as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended.

We will post this report to our website at http://www.epa.gov/oig.

Table of Contents

Chapters

Appendices

Chapter 1
Introduction

Purpose

The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), sought to determine whether the EPA implemented management control processes for maintaining the quality of data in Xacta.

Background

In accordance with the Federal Information Security Management Act of 2002 (FISMA), federal agencies are required to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. FISMA requires agencies to:

- Maintain an inventory of information systems that are operated by, or on behalf of the agency.
- Assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems.
- Determine the level of information security appropriate to protect such agency information and information systems in accordance with standards promulgated by the National Institute of Standards and Technology (NIST).
- Maintain up-to-date system security plans that document the organization's strategy for reducing risk to an acceptable level and to authorize systems to operate based on that strategy.
- Periodically test and evaluate information security controls and techniques to ensure that they are effectively implemented.

Under FISMA, agencies are annually required to report on the adequacy and effectiveness of its information security policies, procedures, practices, and compliance with the requirements.

The EPA implemented Xacta to be the EPA's official system for recording and maintaining information about the agency's compliance with mandated information system security requirements, and includes applications used by EPA for the protection of human health and the environment. Xacta:

- Stores agency-required information system documentation (artifacts) that supports the actions taken by the EPA to comply with mandated security controls.

- Provides status tracking of data related to artifacts (date entered or modified).
- Maintains information systems' authorization to operate documentation reviewed and approved by the Authorizing Official.
- Maintains information regarding security control testing of the agency's information technology assets.
- A POA&M tracks EPA actions to remediate information system security weaknesses.

Maintaining effective data quality in Xacta is important because it serves as the agency's official information system security assessment and weakness tracking record. As such, Xacta provides the data needed for external reporting to the Office of Management and Budget, as well as the data used internally for providing information to senior agency officials on the effectiveness of the EPA's information security program.

Prior to implementing Xacta, the EPA used Automated System Security Evaluation and Remediation Tracking (ASSERT) for the same purpose.

Responsible Office

The Office of Environmental Information' (OEI's) mission is to lead EPA's information management and information technology programs to provide the information, technology and services necessary to advance the protection of human health and the environment. OEI is the office responsible for Xacta. Within OEI, the Senior Agency Information Security Officer (SAISO) is the Xacta system owner. The SAISO is responsible for establishing and managing the agency's information security framework and corresponding roles and responsibilities; and monitoring and reporting on the status of the EPA's information technology security to agency management and other federal entities.

Designated points of contact within each EPA program and regional office use Xacta to report on the offices' compliance with the requirements outlined in FISMA and the EPA's information security program.

Scope and Methodology

We conducted this audit from February 2014 to July 2015. We performed this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives.

We met with the SAISO and the EPA support contractor to OEI to gather an understanding of Xacta's system security documentation, policy and procedures, training, and office organizational structure.

We reviewed guidance issued by the Office of Management and Budget and special publications issued by NIST to determine whether the EPA implemented selected security controls regarding System Authorization and System Security Plans in accordance with federal guidance. We evaluated the EPA's implementation of information system security controls through inquiry, observation and review of documentation.

We reviewed agency policies and procedures related to the maintenance of Xacta data. We judgmentally selected five systems from a listing of 52 EPA systems that Xacta identified as having a security controls assessment performed in fiscal year 2013. We reviewed the Xacta project folders for these five systems and verified that Xacta contained complete and current information documenting compliance with federal guidance and the OEI SAISO's Assessment Projects Reports for the following areas:

- Risk Assessments.
- Security Evaluation/Level.
- Security Controls Assessment Status.
- System Security Plans.

We judgmentally sampled 20 of 823 potential vulnerabilities identified as high-risk on scan reports that were provided by the SAISO's office. The vulnerabilities were identified during a scan conducted by the SAISO office. We did not perform any independent vulnerability scans to validate the existence of the high-risk vulnerabilities documented in the SAISO file. We contacted agency personnel to determine whether the vulnerabilities have been remediated or whether a POA&M had been created in Xacta to track and manage the scan results.

Prior Reporting

We followed up on the five recommendations contained in OIG Briefing Report No. 10-P-0058, *Self-reported Data Unreliable for Assessing EPA's Computer Security Program*, dated February 2, 2010. Our report reviewed the quality of data in the EPA's information system security assessment and weakness tracking system - ASSERT.[1] We determined that the EPA's oversight and monitoring procedures for ASSERT resulted in:

- Unsubstantiated responses for self-reported information.
- Limited reviews and follow-up that inhibited the ability to identify and correct inaccuracies.
- Survey responses regarding the level of training, guidance, and management support for self-reporting system security information

[1] ASSERT was the EPA's official information system security assessment and weaknesses tracking reporting system prior to the agency implementing Xacta. Xacta provides the functionality previously provided by ASSERT.

disclosed that respondents believed more training was needed and they felt pressured to answer system security questions in ASSERT in a positive way.

We recommended that the EPA issue a memorandum to the assistant and regional administrators emphasizing the importance of ensuring personnel accurately assess and report information in ASSERT. We also recommended that the EPA 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 and implement a process to verify that agency security plans incorporate all the minimally required system security controls. The agency agreed with our findings and recommendations.

We collected evidence from the EPA indicating actions were taken to address the previous report recommendations. We relied on data the EPA entered in its Management Audit Tracking System to determine when management indicated that they had completed the corrective actions. All corrective actions were reported as completed by August 2011. Regardless, the agency was not able to provide supporting evidence that they had provided the agreed-to recommended training on how to assess and document the implementation of minimum required security controls.

Chapter 2
Xacta Is Operating With Incomplete and Unapproved System Documentation

Xacta is operating with an Authorization to Operate (ATO) that has expired. Furthermore, the EPA has not completed or approved required system documentation for it. There is no documentation that the current system security plan has been reviewed by management. Also, the Xacta Contingency Plan is incomplete and has not been approved. Further, a required business impact analysis was not performed prior to it receiving an ATO. As required in the temporary authorization, Xacta has not been reauthorized. The federal government and the EPA provide guidance for authorizing systems and maintaining system documentation. The documentation was neither complete nor approved and the reauthorization was not performed because agency personnel are not following federal and agency guidance; the agency did not make it priority to maintain system documentation; and the agency lacks a process to ensure that information systems receiving a temporary authorization to operate are reauthorized.

As a result, the agency is less able to protect and recover system functionality or identify and prioritize information systems and components critical to supporting the organization's mission/business processes. Additionally, the EPA has no assurance that Xacta is operating within management's acceptable level of risks.

Required System Documentation Is Incomplete and Unapproved

There is no documentation that the current Xacta system security plan version 1.4, dated February 2014, has been reviewed by management. An independent contractor for OEI in a Security Assessment Report also identified and documented that the previous plan, version 1.3, was also not reviewed by management. The Xacta Contingency Plan is incomplete and has not been approved. A business impact analysis was not performed prior to Xacta receiving an ATO, as required by NIST and EPA guidance. Specifically, Xacta received its temporary ATO on September 6, 2012. A business impact analysis document was created on April 5, 2011, however, it was incomplete and did not contain all the information required by NIST and EPA guidance. A complete business impact analysis was not performed until April 30, 2014.

According to Office of Management and Budget Circular A-130 Appendix III, *Security of Federal Automated Information Resources*, the security plan shall be consistent with guidance issued by NIST. According to NIST Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, procedures should require that the system security plan be prepared and reviewed prior to proceeding with the security certification and accreditation

process for the system. The EPA's *Information Security Interim Planning Procedures V3.6* requires the document review history be updated to reflect the actual date the review of the security plan was performed and must be signed and approved by a management official.

In addition, NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, requires the contingency plan be developed, tested and approved. This special publication and EPA Chief Information Officer (CIO) *Interim Contingency Planning Procedures V3.2* CIO-2150.3-P.06.1, both require a business impact analysis be conducted and documented prior to development of a contingency plan.

These system document deficiencies occurred because EPA officials used resources for other projects. The EPA has since assigned resources to the preparation of Xacta system documentation.

Not having complete, reviewed and approved information system documentation could affect the ability to (1) improve the protection of the information system resources; (2) recover system functionality in the most expedient and cost-beneficial method; and (3) identify and prioritize information systems and components critical to supporting the organization's mission/business processes to protect human health and the environment.

Xacta Has Not Been Reauthorized to Operate

Xacta is being used in production, although it has not been reauthorized as required. Xacta received a temporary ATO and security authorization on September 6, 2012, as a pilot system. The security authorization and temporary ATO memorandum required that Xacta be reauthorized within 120 days after temporary authorization was received. No reauthorization has occurred.

NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* specifies that the ATO is an official management decision given by an authorizing official (a senior EPA official) to authorize operation of an information system and to explicitly accept the risk to agency operations and agency assets. NIST states that the information system is authorized to operate for a specified time period in accordance with the terms and conditions established by the authorizing official; and that the authorizing official verifies on an ongoing basis that the terms and conditions established as part of the authorization are being followed by the information system owner. The EPA's CIO *Information Security, Interim Security Assessment and Authorization Procedures*, CIO-2150-3-P-04-1, requires an ATO to be signed after an authorizing official certifies that the system has met all the requirements to become operational.

Xacta is being utilized with an expired ATO because the system owner thought the ATO was valid for three years. As such, we could not find where efforts were taken to monitor the temporary ATO to ensure Xacta was reauthorized. Not reauthorizing Xacta means that the EPA cannot certify that it is still operating at an acceptable level of risk.

Conclusion

Senior agency officials' ability to make risk-based decisions is hampered. Xacta could present unknown harm to the EPA's network because management lacks complete information on the system's weaknesses that could negatively impact the organization's mission/business processes to protect human health and the environment.

Recommendations

We recommend that the Chief Information Officer, Office of Environmental Information:

1. Develop information system documentation for Xacta to comply with federal and agency guidelines.

2. Complete reauthorization of Xacta as required by the temporary authorization to operate, dated September 6, 2012.

3. Conduct and document a review of the EPA's process to reauthorize information systems that received a temporary authorization to operate and update the procedures as needed.

Agency Response to Draft Report and OIG Evaluation

The agency agreed with the report findings and provided documentation to support that it completed corrective actions for recommendations 1 and 2. We believe the response to these two recommendations fully address our concerns, and we consider these recommendations closed with all agreed-to actions completed.

In response to Recommendation 3, OEI indicated requirements are in place to re-authorize or decommission or otherwise halt operations for systems that do not have a current authorization regardless of the length of time of an authorization. OEI also provided documentation to support that a process is in place to review authorizations monthly. However, we believe this process failed to identify that Xacta required an authorization to operate and to ensure management took steps to correct the deficiency. As such, we expressed concerns that OEI should conduct a review of its implemented process to ensure it is appropriately designed

and working as intended. Upon further discussions with OEI, the office provided documentation to support that, subsequent to us issuing our draft report, management completed a review of the process used to re-authorize systems without current authorizations to operate. We believe the response and subsequent actions fully address our concerns, and we consider this recommendation closed with all agreed-to actions completed. Appendix A contains OEI's response and Appendix B contains OEI's revised corrective actions.

Chapter 3
EPA Needs to Improve Remediation and Management of Known Vulnerabilities

The EPA's network is exposed to known vulnerabilities which are not being tracked and managed in Xacta. EPA information security documents require all findings and vulnerabilities be tracked within Xacta. Agency security personnel are not taking immediate steps to develop a POA&M in Xacta to track and manage identified vulnerabilities. The EPA has not created a reporting mechanism that informs the assistant and regional administrators about un-remediated vulnerabilities or holds senior personnel accountable for taking corrective actions. As a result, the EPA's information technology assets and data may unnecessarily be exposed to risks without senior management knowledge or a plan to correct the deficiency.

High-Risk Vulnerabilities Remain Unresolved and Not Tracked

Agency personnel are not tracking and managing known high-risk vulnerabilities within Xacta to protect the agency's network. As of February 2014, the SAISO office's network scans listed 823 potential high-risk vulnerabilities that have not all been remediated nor had a POA&M entered in Xacta. The SAISO's report indicates that some of these vulnerabilities have remained unresolved between 90 to 340 days since originally reported to agency personnel for remediation.

EPA Procedure CIO-2150-3-P-04.1 requires all findings of weaknesses and recommendations be tracked with a POA&M and entered in Xacta. Additionally, EPA Procedure, *Information Security – Interim Risk Assessment Procedure V.3.4*, CIO-2150.3-P-14.1, requires high-risk vulnerabilities discovered from vulnerability and penetration testing to be remediated within 30 days.

We judgmentally sampled 20 of the 823 potential vulnerabilities identified as high-risk on scan reports that were being tracked by the SAISO's office. We found that prior to our inquiry, 45 percent (9 of 20) of the vulnerabilities were either remediated or a POA&M was entered in Xacta. However, the EPA:

- Entered a POA&M in Xacta for 40 percent (8 of 20) of the vulnerabilities after our inquiry.
- Had not entered a POA&M in Xacta for 15 percent (3 of 20) of the vulnerabilities and no plan exists to create a POA&M.

We learned from agency personnel that some of the sampled potential vulnerabilities were not remediated or did not have a POA&M entered in Xacta because personnel:

1) Were still investigating the nature of the potential vulnerability even after being notified by the SAISO's office several months prior to the potential vulnerability's discovery.
2) Decided to track and manage the vulnerability within the agency's vulnerability scanning tool instead of Xacta to reduce administrative efforts.
3) Had expired security tokens preventing access to Xacta to record a POA&M.
4) Lacked the necessary training to use Xacta for data entry.

The SAISO's office established a process where monthly security reports documenting high-risk vulnerabilities requiring remediation are sent to agency senior information officials and primary information security officers. The monthly security report further contains instructions to coordinate with respective agency personnel responsible for implementing and maintaining information security controls to develop a POA&M for high-risk vulnerabilities not addressed within 30 days. High-risk vulnerabilities remain un-remediated because agency personnel are not taking the necessary steps to ensure, at a minimum, that a POA&M is entered in Xacta to track and manage the known vulnerability, even in those instances where personnel cannot immediately remediate the vulnerability.

In response to our discussion document, outlining our potential findings, OEI implemented a reporting mechanism requesting senior officials' involvement to resolve metrics that are rated substandard. However, we determined that the new reporting process does not (1) inform assistant and regional administrators about un-remediated known high-risk vulnerabilities and (2) hold the senior information officials and primary information security officers accountable for taking corrective actions.

Failure to create a timely POA&M to manage known high-risk vulnerabilities could lead to the exploitation of information technology resources and adversely affect the responsiveness of the agency's information security program to security events.

Conclusion

Managing and tracking of information security vulnerabilities are paramount in protecting the agency's information security posture. Any deficiencies in information security practices hinder the agency's ability to monitor the current operational status of the EPA's network infrastructure and ensure the security of information technology resources that are necessary to advance the protection of human health and the environment.

Recommendations

We recommend that the Chief Information Officer, Office of Environmental Information:

4. Develop and implement a process using Xacta to manage vulnerabilities, especially high-risk vulnerabilities that could impact the agency's infrastructure and information technology resources.

5. Direct the SAISO to finalize efforts to set Xacta standards and implement Xacta support to simplify most users' tasks within the system.

Agency Response to Draft Report and OIG Evaluation

The agency agreed with the report findings and provided documentation to support that it completed corrective actions for recommendation 4. We believe the response to recommendation 4 fully addresses our concerns, and we consider this recommendation closed with all agreed-to actions completed.

In response to Recommendation 5, OEI indicated that it took steps to address the recommendation. OEI also outlined further actions it is undertaking to periodically canvass EPA headquarters and regional security personnel to determine training needs and to provide Xacta training, as needed. We believed OEI will fully address our concerns once it completes the remaining planned actions. Upon further discussions with OEI, we modified recommendation 5 to clarify our concerns. The agency agreed with the revised recommendation and provided planned dates for completing corrective actions. We consider recommendation 5 open with agreed-to corrective actions pending.

Appendix A contains OEI's response and Appendix B contains OEI's revised corrective actions.

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	7	Develop information system documentation for Xacta to comply with federal and agency guidelines.	C	Chief Information Officer, Office of Environmental Information	9/24/14		
2	7	Complete reauthorization of Xacta as required by the temporary authorization to operate, dated September 6, 2012.	C	Chief Information Officer, Office of Environmental Information	2/3/15		
3	7	Conduct and document a review of the EPA's process to reauthorize information systems that received a temporary authorization to operate and update the procedures as needed.	C	Chief Information Officer, Office of Environmental Information	8/5/15		
4	11	Develop and implement a process using Xacta to manage vulnerabilities, especially high-risk vulnerabilities that could impact the agency's infrastructure and information technology resources.	C	Chief Information Officer, Office of Environmental Information	6/2/15		
5	11	Direct the SAISO to finalize efforts to set Xacta standards and implement Xacta support to simplify most users' tasks within the system.	O	Chief Information Officer, Office of Environmental Information	12/31/16		

[1] O = Recommendation is open with agreed-to corrective actions pending.
C = Recommendation is closed with all agreed-to actions completed.
U = Recommendation is unresolved with resolution efforts in progress.

OEI Response to Draft Report

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

AUG 31 2015

OFFICE OF
ENVIRONMENTAL INFORMATION

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OA-FY14-0078 "*EPA Needs to Improve Security Planning for Its Risk Management System and Improve Processes for Remediating Known Weaknesses*," dated July 28, 2015

FROM: Ann Dunkin
Chief Information Officer

TO: Arthur A. Elkins, Jr.
Inspector General

Thank you for the opportunity to respond to the issues and recommendations for the draft report "*EPA Needs to Improve Security Planning for Its Risk Management System and improve Processes for Remediating Known Weaknesses*."

AGENCY'S OVERALL POSITION: OEI feels that all of the recommendations in this Draft Audit Report have been addressed. In the attached table, we have noted the actions taken and the dates the actions were completed. We have also provided files or links to document how we addressed those actions.

If you have any questions regarding this response, please contact OEI's Audit Follow-up Coordinator, Judi Maguire at maguire.judi@epa.gov or (202)564-7422.

Attachments

cc: Rudy Brevard
Albert Schmidt
Bettye Bell-Daniel
Nicholas Grzegozewski
Judi Maguire
Kevin Donovan
Renee Gutshall
Brenda Young

OEI's Response to the Recommendations

No.	Recommendation	High Level Intended Corrective Action
1	We recommend that the Chief Information Officer for the Office of Environmental Information develop information system documentation for Xacta to comply with federal and agency guidance.	OEI believes this recommendation is not applicable. The Xacta Information Assurance Manager Application has a complete authorization package in place. **Completion date: 9/24/2014** **Artifact: Refer to the XACTA tool for information system documentation https://xacta.epa.gov**
2.	Complete reauthorization of Xacta as required by the temporary authorization to operate dated September 6, 2012.	OEI believes this recommendation is not applicable. The XACTA Information Assurance Manager Application has a current full ATO. **Completion date: 02/03/2015** **Artifact: Memo – Authorization to Operate for the XACTA IAM Application**
3.	Implement a process to reauthorize information systems that received a temporary authorization to operate.	OEI believes this recommendation is not applicable. Requirements are in place to re-authorize or decommission or otherwise halt operations for systems that do not have a current authorization regardless of the length of time of an authorization. A process is in place to review authorizations monthly. Review results are promulgated to senior leaders, IT managers and information security personnel by the CIO. Senior leaders, IT managers and information security personnel are to respond to the CIO with corrective actions for any discrepancies noted in the reports. **Complete: 11/15/2011** **Artifact: ATO Report Nov 15 2011.xlsx**

4.	Develop and implement a process using Xacta to manage vulnerabilities, especially "high-risk" vulnerabilities that could impact the agency's infrastructure and information technology resources.	OEI believes this recommendation is not applicable. Processes exist to manage vulnerabilities. Xacta is one of the tools used and its use is documented. **Complete: 6/2/2015, Artifact: Xacta_POA_M_Guide.pdf, CIO-2151-3-P-04-1.pdf (Interim Assessment and Authorization Procedures), CIO-2150-3-P-14-1.pdf (Interim RA Procedure), CIO-2150-3-P-01-1.pdf (Interim Access Control Procedures) for procedures http://intranet.epa.gov/oei/imitpolicy/policies.htm**
5.	Direct the SAISO to periodically canvass EPA headquarters and regional security personnel to determine training needs on how to use Xacta and conduct training accordingly.	OEI believes this recommendation is not applicable. The SAISO holds monthly calls with all ISOs to discuss many issues to include training. A tiger team was established to look at Xacta processes and training. Xacta training was purchased from the tool vendor and made available through eLearning. Xacta training was provided at the 2015 Information Security Summit and is provided to users as needed. In addition, the SAISO is working with an ISO workgroup to set standards in regards to training and implement Xacta support to simplify most users' tasks with Xacta under the mandate of an Information Security Task Force (ISTF). **Complete: 2/26/2015 Artifact: Rec5_eLearningScreenshotsXACTAtraining.docx**

Appendix B

Agreed-to Revised Corrective Actions

No.	Recommendation	High Level Intended Corrective Action
1	We recommend that the Chief Information Officer for the Office of Environmental Information develop information system documentation for Xacta to comply with federal and agency guidance.	OEI believes this recommendation is not applicable. The Xacta Information Assurance Manager Application has a complete authorization package in place. **Completion date: 9/24/2014** **Artifact: Refer to the XACTA tool for information system documentation https://xacta.epa.gov**
2.	Complete reauthorization of Xacta as required by the temporary authorization to operate dated September 6, 2012.	OEI believes this recommendation is not applicable. The XACTA Information Assurance Manager Application has a current full ATO. **Completion date: 02/03/2015** **Artifact: Memo – Authorization to Operate for the XACTA IAM Application**
3.	Conduct and document a review of EPA's process to reauthorize information systems that received a temporary authorization to operate and update the procedures as needed.	We have a process in place for temporary ATO's within the Agency. The Interim Security Assessment and Authorization procedure addresses this process. We are currently awaiting approval for the interims. Monthly information security reports are provided to show senior leaders system status. A POA&M guide is also provided to users as an additional insight to the process. **Complete: 8/5/2015** **Artifacts: Enterprise Infosec Status Report June 2015.pdf, Enterprise Infosec Status - Executive Report - July 2015.pdf, Xacta_POA_M_Guide.pdf, CIO-2150-3-P-04-1.pdf (Interim Security Assessment and Authorization Procedure)**
4.	Develop and implement a process using Xacta to manage vulnerabilities, especially "high-risk" vulnerabilities that could impact the agency's	OEI believes this recommendation is not applicable. Processes exist to manage vulnerabilities. Xacta is one of the tools used and its use is documented. **Complete: 6/2/2015,** **Artifact: Xacta_POA_M_Guide.pdf, CIO-2151-3-P-04-1.pdf (Interim Assessment and Authorization Procedures), CIO-2150-3-P-14-1.pdf (Interim RA Procedure), CIO-2150-3-P-01-1.pdf (Interim Access**

No.	Recommendation	High Level Intended Corrective Action
	infrastructure and information technology resources.	**Control Procedures) for procedures http://intranet.epa.gov/oei/imitpolicy/policies.htm**
5.	Direct the SAISO to finalize efforts to set Xacta standards and implement Xacta support to simplify most users' tasks within the system.	**We are planning on having the service in place by end of 1st qtr FY17.**

Appendix C

Distribution

Office of the Administrator
Chief Information Officer
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Principal Deputy Assistant Administrator for Environmental Information and Deputy Chief Information Officer
Audit Follow-Up Coordinator, Office of Environmental Information