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.