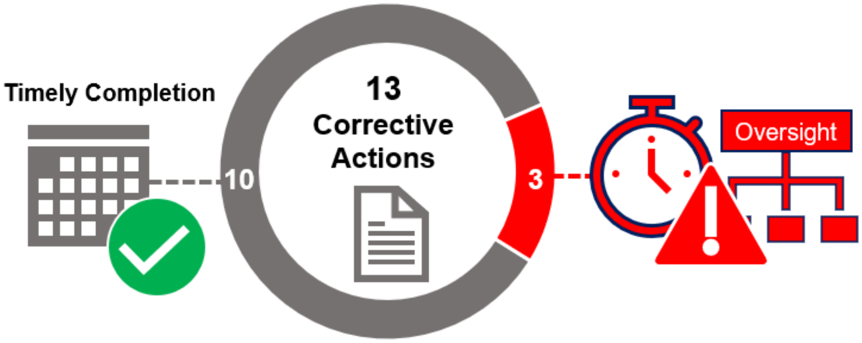
OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

CUSTOMER SERVICE ★ INTEGRITY ★ ACCOUNTABILITY

Operating efficiently and effectively

EPA Generally Adheres to Information Technology Audit Follow-Up Processes, but Management Oversight Should Be Improved

Report No. 22-P-0010 **December 8, 2021**



Report Contributors:

LaSharn Barnes
LaVonda Harris-Claggett
Eric Jackson Jr.
Alonzo Munyeneh
Jeremy Sigel
Sabrena Stewart

Abbreviations:

EPA	U.S. Environmental Protection Agency
FY	Fiscal Year
IT	Information Technology
OCSPP	Office of Chemical Safety and Pollution Prevention
OIG	Office of Inspector General
OMB	Office of Management and Budget
OMS	Office of Mission Support
OPP	Office of Pesticide Programs
PRISM	Pesticide Registration Information System
RBT	Role-Based Training
U.S.C.	United States Code

Cover Image: The EPA completed the 13 corrective actions we reviewed as part of this audit; however, discrepancies related to a lack of management oversight were found in three of the 13 corrective actions. (EPA OIG image)

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, D.C. 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

Office of Inspector General
U.S. Environmental Protection Agency

At a Glance

22-P-0010
December 8, 2021

Why We Did This Audit

The Office of Inspector General conducted this audit to determine whether the (1) U.S. Environmental Protection Agency completed corrective actions for agreed-to cybersecurity audit recommendations in OIG reports issued from fiscal year 2017 through fiscal year 2020 and (2) corrective actions effectively resolved the weaknesses identified.

The OIG has identified *Enhancing Information Technology Security to Combat Cyberthreats* as a key management challenge confronting the EPA. The OIG has a responsibility to detect and prevent mismanagement and misconduct in the EPA's programs and operations. The OIG achieves this, in part, by confirming that agreed-to corrective actions to address OIG report recommendations and findings were completed by the Agency.

This audit supports an EPA mission-related effort:

- *Operating efficiently and effectively.*

This audit addresses top EPA management challenges:

- *Enhancing information technology security.*
- *Complying with key internal control requirements (data quality; policies and procedures).*

Address inquiries to our public affairs office at (202) 566-2391 or OIG_WEBCOMMENTS@epa.gov.

List of OIG reports.

EPA Generally Adheres to Information Technology Audit Follow-Up Processes, but Management Oversight Should Be Improved

What We Found

The EPA completed the 13 corrective actions for cybersecurity audit recommendations in the OIG reports that we reviewed as part of this audit. However, for one of the 13 corrective actions, the EPA inaccurately reported its timely completion. For two of the 13 corrective actions, the EPA lacked management oversight to effectively resolve identified weaknesses. We found that the EPA has deficiencies in the following areas:

The EPA's goal to provide its workforce and the public with accurate information is undermined when the Agency does not correct deficiencies in a timely manner, which weakens the integrity of its systems and data.

- Verifying compliance with annual training requirements for information technology contractors with significant information security responsibilities.
- Verifying corrective actions were completed as represented by the Agency.
- Deploying patches to mitigate identified vulnerabilities in the Agency's Pesticide Registration Information System database in a timely manner.

Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Chemical Safety and Pollution Prevention develop a strategy to validate that corrective actions are completed before closing them in the Agency's audit tracking system and implement controls to comply with federal and Agency required time frames to install patches. In addition, we recommend that the assistant administrator for Mission Support develop and implement processes for storing certifications collected for annual role-based training requirements in a centralized restricted location.

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

—National Institute of Standards and Technology's *Glossary*

The EPA agreed with our four recommendations; completed corrective actions for two of them; and provided acceptable planned corrective actions and estimated milestone dates for the remaining two, which we consider resolved with corrective actions pending.

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

THE INSPECTOR GENERAL

December 8, 2021

MEMORANDUM

SUBJECT: EPA Generally Adheres to Information Technology Audit Follow-Up Processes,
but Management Oversight Should Be Improved
Report No. 22-P-0010

FROM: Sean W. O'Donnell Sean W O'Donnell

TO: Michal Ilana Freedhoff, Assistant Administrator
Office of Chemical Safety and Pollution Prevention

Lynnann Hitchens, Acting Principal Deputy Assistant Administrator
Office of Mission Support

This is our report on the subject audit conducted by the U.S. Environmental Protection Agency's Office of Inspector General. The project number for this audit was OA-FY21-0067. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The EPA's Office of Chemical Safety and Pollution Prevention and Office of Mission Support are responsible for the issues discussed in this report.

We issued four recommendations in this report. The Office of Chemical Safety and Pollution Prevention completed corrective actions for one of the recommendations and provided acceptable planned corrective actions for two recommendations. The Office of Mission Support completed corrective actions for one of the recommendations. In accordance with EPA Manual 2750, all recommendations are completed or resolved with corrective actions pending. No final response to this report is required. However, if you submit a response, it will be posted on the OIG's website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

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

Table of Contents

Chapters

Appendixes

Chapter 1
Introduction

Purpose

The U.S. Environmental Protection Agency's Office of Inspector General initiated this audit to determine whether the (1) EPA completed corrective actions for agreed-to cybersecurity audit recommendations in OIG reports issued from fiscal year 2017 through FY 2020 and (2) actions taken by the EPA effectively resolved the weaknesses identified in the selected audit reports.

Top Management Challenges Addressed

This audit addresses the following top management challenges for the Agency, as identified in OIG Report No. 20-N-0231, *EPA's FYs 2020–2021 Top Management Challenges*, issued July 21, 2020:

- Enhancing information technology security.
- Complying with key internal control requirements (data quality; policies and procedures).

Background

The Reports Consolidation Act of 2000 (31 U.S.C. § 3516(d)) requires that the OIG prepare an annual report summarizing what it considers the "most serious management and performance challenges facing the agency." Identifying and resolving top management challenges are essential to the EPA's mission of protecting human health and the environment. Since 2013, the EPA's OIG has identified *Enhancing Information Technology Security to Combat Cyberthreats* as a key management challenge confronting the EPA. In addition, it is the OIG's responsibility to detect and prevent mismanagement and misconduct in EPA programs and operations. The OIG achieves this, in part, by confirming if agreed-to corrective actions that address OIG report recommendations and findings have, in fact, been completed by the Agency. Those found not to be completed are then reported in the OIG's *Semiannual Report to Congress* in the "Status of OIG Unimplemented Recommendations" section.

The OIG conducted a prior audit—Report No. 16-P-0100, *EPA Needs to Improve Its Information Technology Audit Follow-Up Processes*, issued March 10, 2016—to review the EPA's actions related to eight OIG audit reports with information technology, or IT, security findings that were issued in FYs 2010–2012 or were associated with the *Enhancing Information Technology Security to Combat Cyberthreats* management challenge. These eight reports contained a total of 65 recommendations. The OIG's analysis of six (or roughly 9 percent) of the 65 recommendations found that the EPA's oversight of the offices reviewed did not ensure that agreed-to corrective actions were:

- Fully implemented.
- Carried out in a timely manner.
- Accurately recorded.
- Effectively managed in the Agency's audit tracking system.

Specifically, this audit determined that corrective actions were not always verified by the Agency, even though the corrective actions were recorded as completed in the Agency's audit tracking system. In addition, we found that the Agency lacked internal controls over its audit follow-up process to promote management accountability for ensuring agreed-to corrective actions were completed as specified in the management's plans.

Office of Management and Budget Circular A-50 Revised, *Audit Followup*, requires each agency to establish follow-up systems that accurately document and record the status of recommendations. OMB Circular A-50 Revised also specifies that:

> The audit followup official has personal responsibility for ensuring that (1) systems of audit followup, resolution, and corrective action are documented and in place, (2) timely responses are made to all audit reports, (3) disagreements are resolved, (4) corrective actions are actually taken, and (5) semi-annual reports … are sent to the head of the agency.

EPA Manual 2750, *Audit Management Procedures*, based in part on OMB Circular A-50 Revised, prescribes the EPA's audit-management and follow-up policies and procedures. It designates the chief financial officer as the Agency audit follow-up official responsible for ensuring that agencywide audit management, audit resolution, and audit follow-up policies and procedures are in place. The Office of the Chief Financial Officer administers the Agency's audit tracking system and uses it to record, track, and report to Congress on the status of OIG recommendations and Agency steps to implement agreed-to corrective actions.

Responsible Offices

The chief financial officer, as the Agency's audit follow-up official, is responsible for agencywide audit resolution. In addition, the chief financial officer is responsible for ensuring that action officials implement agreed-to corrective actions.

The administrator, the general counsel, and each assistant administrator and regional administrator designate an audit management official for their offices who is responsible for designating an office audit follow-up coordinator. We reviewed recommendations related to IT processes made to the Office of Mission Support, or OMS; Office of Chemical Safety and Pollution Prevention, or OCSPP; and Office of Land and Emergency Management. The audit follow-up coordinators for these offices are responsible for coordinating audit management activities within their organizations and for maintaining records and entering data on audit follow-up activities in the Agency's audit tracking system.

The Agency's audit follow-up coordinator in the Office of the Chief Financial Officer performs the following functions:

- Supports the Agency audit follow-up official.
- Monitors the implementation status of corrective actions in the audit tracking system.
- Provides guidance and assistance to office audit follow-up coordinators in each national program and regional office on audit follow-up procedures.

Scope and Methodology

We conducted this performance audit from December 2020 through August 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objective.

To address our audit objectives, we performed an analysis of 17 cybersecurity audit reports issued by the OIG from FY 2017 through FY 2020. These reports contained a total of 62 recommendations with corresponding corrective actions agreed to by the Agency. As part of that analysis we:

- Reviewed the "Status of Recommendations and Potential Monetary Benefits" tables from the 17 prior audit reports to identify the status of recommendations and the associated corrective action completion dates.

- Identified which of the 17 audit reports had recommendations tracked and followed up on in other OIG reports, such as the financial statement or Federal Information Security Modernization Act audits.

- Reviewed the Agency's responses to the final reports and any subsequent responses detailing the proposed corrective actions to identify which recommendations were completed and which corrective actions were past due.

As a result of this analysis, we identified 31 recommendations from seven different audit reports consisting of 13 corrective actions reported by the Agency as completed and two corrective actions that were not yet past due but were proposed to be completed by December 31, 2020, for a total of 15 corrective actions selected for review (Table 1). Following this audit's entrance conference, the estimated completion dates for the two corrective actions due by December 31, 2020, were extended beyond our fieldwork time frame in compliance with EPA Manual 2750 requirements, leaving 13 in-scope corrective actions reviewed. See Appendix A for a complete list of OIG report recommendations and the associated corrective actions that we reviewed.

Table 1: OIG audit reports and recommendations

OIG report number	Report title	Date issued	Number of recommendations with corresponding corrective actions	Number of recommendations whose corrective actions' estimated completion dates have passed
17-P-0029	*Acquisition Certifications Needed for Managers Overseeing Development of EPA's Electronic Manifest System*	11/7/16	2	1
18-P-0298	*Management Alert: EPA's Incident Tracking System Lacks Required Controls to Protect Personal Information*	9/28/18	4	4
19-P-0158	*Insufficient Practices for Managing Known Security Weaknesses and System Settings Weaken EPA's Ability to Combat Cyber Threats*	5/21/19	3	2*
19-P-0195	*Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement*	6/21/19	7	3

OIG report number	Report title	Date issued	Number of recommendations with corresponding corrective actions	Number of recommendations whose corrective actions' estimated completion dates have passed
17-P-0344	*EPA Lacks Processes to Validate Whether Contractors Receive Specialized Role-Based Training for Network and Data Protection*	7/31/17	4	3
20-P-0007	*Management Alert: EPA Still Unable to Validate that Contractors Received Role-Based Training for Information Security Protection*	10/21/19	4	1
20-E-0309	*EPA Needs to Improve Processes for Securing Region 8's Local Area Network*	9/10/20	7	1*
Total recommendations			**31**	**13**

Source: OIG analysis. (EPA OIG table)

*This number includes one recommendation whose estimated completion was extended beyond our fieldwork time frame and, therefore, was not included in the total.

We obtained documentation supporting all 13 completed corrective actions. Based on our analysis of the documentation received, we determined which actions had in fact been completed as stated by the Agency. If the supporting documentation and our analysis did not show the corrective actions as complete, we did not conduct any further follow-up.

We then selected three audit recommendations to evaluate whether the underlying issues were resolved by the Agency's actions. For two of the recommendations related to IT contract acquisition, we selected five contracts from a list of IT contracts from FY 2020 through FY 2021. We chose five contracts, which consisted of the four contracts with the highest values and documentation of having assigned contracting officer representatives and one contract with the highest value listed for a contract without such documentation. For the remaining recommendation related to patch management, we obtained support relevant to the release and installation of the bundle patch for the Agency's Oracle Database Appliance software. We calculated the time between the patch's release by the vendor to the installation by the Agency and analyzed the results.

Patch management is the process of distributing and applying updates to software. These patches are often necessary to correct errors (also referred to as "vulnerabilities" or "bugs") in the software.

A ***bundle patch*** is a cumulative collection of fixes for a specific product or component.

Chapter 2

EPA Inaccurately Reported Timely Completion for One of 13 Corrective Actions Reviewed

The EPA claimed completion of corrective actions for the 13 cybersecurity audit recommendations we reviewed. However, for one of the 13 corrective actions reviewed, we found that the EPA inaccurately reported timely completion in the Agency's tracking system before the actions were completed. Specifically, the OCSPP reported completion of the corrective action related to updating patch-management procedures 16 months before the action was actually completed. This erroneous reporting occurred because the program manager responsible for implementing the action informed the OPP audit follow-up coordinator that the action had been completed even though the vulnerability remediation time frames had not been updated in accordance with the corrective action. EPA guidance requires Agency managers to verify that corrective actions are completed and include progress, status, delays, and completion dates in the Agency's audit tracking system. Inaccurate data in the Agency's audit tracking system can mislead the public and limit the OIG's assurance that the OIG can rely on the corrective actions reported by the Agency.

The EPA's ***PRISM*** provides a central location to securely access documentation and reports supporting various aspects of the pesticide regulatory process.

The OCSPP reported completion of the corrective action to address Recommendation 4 of OIG Report No. 19-P-0195, *Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement*, issued June 21, 2019, in the Agency's audit tracking system 16 months before the actions were actually completed. In the corrective action plan, the OCSPP concurred with the recommendation and indicated that the Office of Pesticide Programs, or OPP, would comply with OMS guidance for federally required time frames to install patches to correct identified vulnerabilities in the Pesticide Registration Information System, among other updates to system security controls. Updates were made to PRISM's *System Security Plan* to fulfill the corrective action addressing the OIG's recommendation, and its completion date was recorded in the Agency's audit tracking system as August 14, 2019. Based on our analysis of the *System Security Plan* dated August 14, 2019, we found that, although updates were made to other relevant security controls in the plan, the patch-management time frames to remediate vulnerabilities did not adhere to Agency requirements; thus, the corrective action had not, in fact, been completed in August 2019 as recorded in the Agency's system. The OCSPP completed the corrective action in December 2020 when it updated the *System Security Plan* to adhere to required time frames. However, the OCSPP did not record the revised completion date in the audit tracking system.

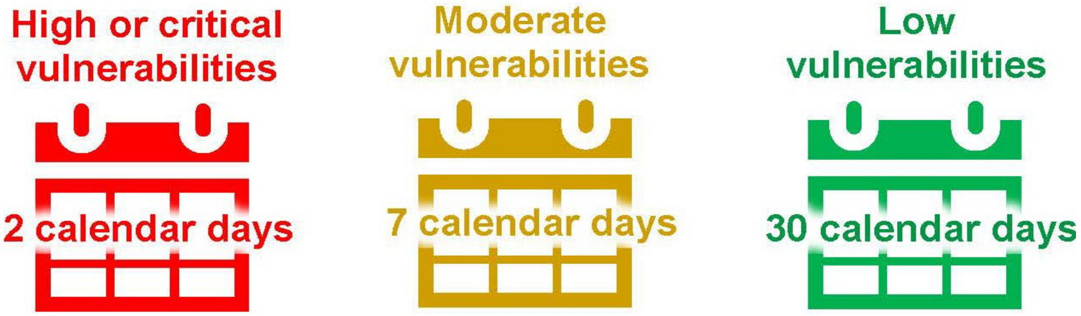
The National Institute of Standards and Technology defines a ***system security plan*** as a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

The OCSPP's OPP was responsible for updating the *System Security Plan* in response to our prior recommendations. The OPP's audit follow-up coordinator contacted the OPP program manager responsible for implementing the corrective action who wrongly confirmed that the action was complete. The OPP audit follow-up coordinator informed the OCSPP audit follow-up coordinator, who is responsible for closing out the corrective action in the Agency's audit tracking system, that the corrective action was completed. The OCSPP audit follow-up coordinator recorded the action as completed based on the information received from the OPP audit follow-up coordinator. The OPP subsequently discovered that PRISM's *System Security Plan* was not updated to comply with the Agency required time frames to remediate vulnerabilities and that the updates were made in December 2020.

Section SI-2 of the National Institute of Standards and Technology's SP 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, states that security-relevant software and firmware updates must be installed within an agency-defined time period after their release. The EPA's CIO Directive No. 2150-P-17.2, *Information Security—Interim System and Information Integrity Procedures,* dated January 2017, defines the following patch-management time frames to remediate vulnerabilities (Figure 1):

- High- or critical-priority vulnerabilities shall be mitigated within two calendar days.
- Moderate-priority vulnerabilities shall mitigated within seven calendar days.
- Low-priority vulnerabilities shall be mitigated within 30 calendar days.

Figure 1: EPA-established patch-management vulnerability-remediation time frames



Source: OIG analysis of CIO Directive No. 2150-P-17.2. (EPA OIG image)

The EPA's documented processes for PRISM were not in compliance with federal and Agency requirements because the EPA did not update the *System Security Plan* for the PRISM application within the established Agency-defined time frames for remediating vulnerabilities.

EPA Manual 2750 requires that the Agency include any progress, status, delay, and completion date in the appropriate fields in the Agency's audit tracking system at least quarterly. Inaccurate and false data in the audit tracking system limit the OIG's assurance that the OIG can rely on the corrective actions reported by the Agency, impact the integrity of the OIG's *Semiannual Reports to Congress*, and can erode public confidence in the Agency's claims that the Agency has fulfilled the corrective actions it pledged to take in response to OIG recommendations.

Recommendations

We recommend that the assistant administrator for Chemical Safety and Pollution Prevention:

1. Update the Agency's audit tracking system with the correct completion dates and reasons for the delays for corrective actions related to Recommendation 4 of EPA OIG Report Number 19-P-0195, *Pesticide Registration Fee, Vulnerability Mitigation and Database Security*

Controls for EPA's FIFRA and PRIA Systems Need Improvement, issued June 21, 2019, as required by EPA Manual 2750, *Audit Management Procedures*.

2. Instruct program managers that they must validate that corrective actions are completed before closing them in the Agency's audit tracking system.

Agency Response and OIG Assessment

The OCSPP concurred with Recommendations 1 and 2; completed corrective actions for Recommendation 1 on September 29, 2021; and provided acceptable planned corrective actions and estimated milestone dates for Recommendation 2. We consider Recommendation 1 completed and Recommendation 2 resolved with corrective actions pending. Appendix B contains the OCSPP's response to the draft report.

Chapter 3

EPA Lacked Management Oversight to Effectively Resolve Weaknesses Identified for Two of 13 Corrective Actions Reviewed

While the OIG verified that the EPA completed corrective actions for the 13 cybersecurity recommendations we reviewed, those actions did not effectively resolve two of the related OIG findings. Specifically, the EPA was unable to verify the certification and preservation of documentation to support IT contractors' compliance with Agency training requirements. In addition, the Agency failed to install security patches for its PRISM production database in accordance with federal and Agency information security directives. These findings occurred because the EPA lacked management oversight to ensure that it stored contractor training requirement documentation in a centralized location and prioritized patch deployment for timely completion. Agency guidance requires that all contractors with information security duties complete training specific to their roles and have certifications proving such. Federal guidance requires organizations to install security-relevant software updates within the time frames that the organization defines. Without assurance that IT contractors with significant security responsibilities comply with Agency training requirements, the EPA risks having contractors with unauthorized access to the Agency's information systems and data. Furthermore, lack of timely mitigation of vulnerabilities via patch deployment may compromise the security and integrity of the Agency's data.

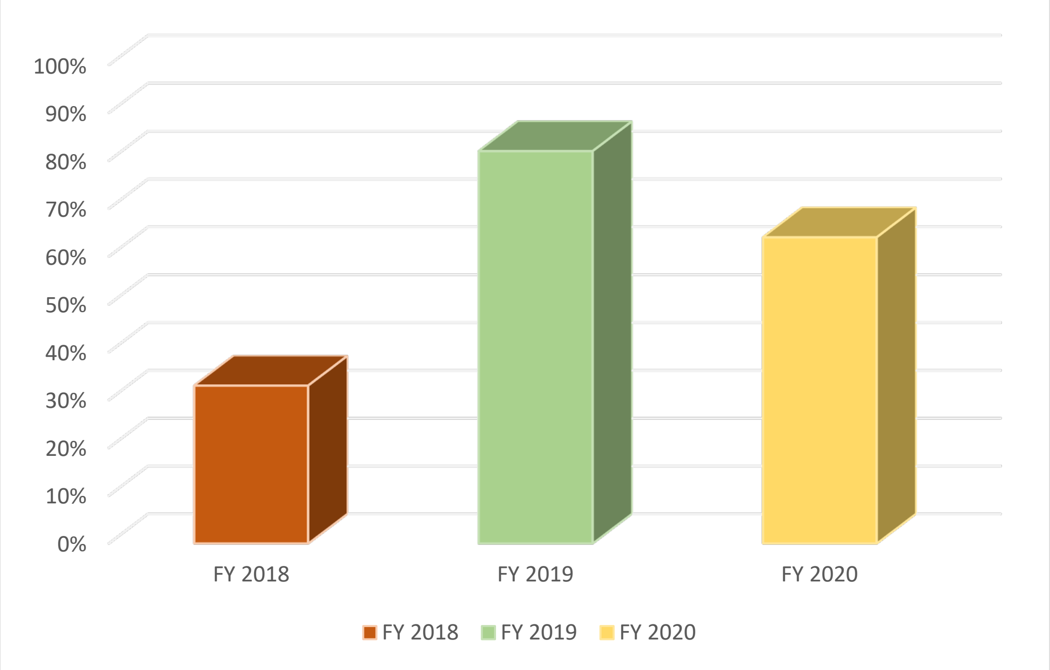
OMS Unable to Support Completion of Regions' and Program Offices' Annual IT Contractor Information Security Training Certifications

The OMS was unable to verify that all ten regions and 12 program offices attested to their IT contractors' completion of role-based training, or RBT, requirements for FYs 2019 and 2020. A previous OIG report—Report No. 20-P-0007, *Management Alert: EPA Still Unable to Validate that Contractors Received Role-Based Training for Information Security Protection,* issued October 21, 2019—found that only seven (or roughly 33 percent) of 21 EPA offices, which at the time did not include the Office of the Administrator, certified that contractor personnel with significant IT responsibilities completed the required RBT. The roles performed by contracting personnel include:

- IT specialists.
- System administrators.
- Network administrators.
- Data loss-prevention specialists.

The OMS distributed a memorandum to the regional and program offices in August 2018 to establish a process for certifying IT contractors' completion of annual RBT requirements. Since the introduction of the process, the OMS has not obtained attestations from all regional and program offices by the established annual deadline of September 30, as shown in Figure 2.

Figure 2: Percentages of EPA offices' RBT attestations submitted by fiscal year



Source: OIG analysis of OMS provided RBT attestation documentation. (EPA OIG image)

For FY 2019, 18 (roughly 82 percent) of 22 EPA offices completed the RBT attestation requirement, with three program offices and one region (about 18 percent) missing completed RBT attestations. For FY 2020, 14 (about 64 percent) of 22 EPA offices completed the RBT attestation requirement, while attestations for six program offices and two regions (roughly 36 percent) were incomplete. While the rate of verified attestations has increased since FY 2018, the EPA is still unable to support full compliance with the Agency's RBT requirements for its contractors.

EPA CIO 2150-P-02.2, *Information Security—Awareness and Training Procedures*, dated February 16, 2016, requires that information security officers "identify all individuals requiring role-based security -related training within their respective program offices or regions" and that senior Agency information security officers ensure "contractors designated as having significant information security responsibilities receive adequate training with respect to such responsibilities."

In addition, the EPA's August 15, 2018 *Certification of Information Security Role -Based Training for Contractor Staff* memorandum requires all senior information officials to provide annual written certification that EPA contractors with information security duties have completed the necessary RBT specific to their contract roles.

The RBT certification process lacked management oversight in that the responses by EPA offices were sent to the chief information security officer's email account without a succession plan for maintaining or transferring this documentation upon the chief information security officer's retirement in December 2020. Furthermore, the EPA lacked management oversight by not establishing a centralized, logically restricted location to store the offices' attestations, which led to confusion among OMS personnel as to the location of all RBT responses.

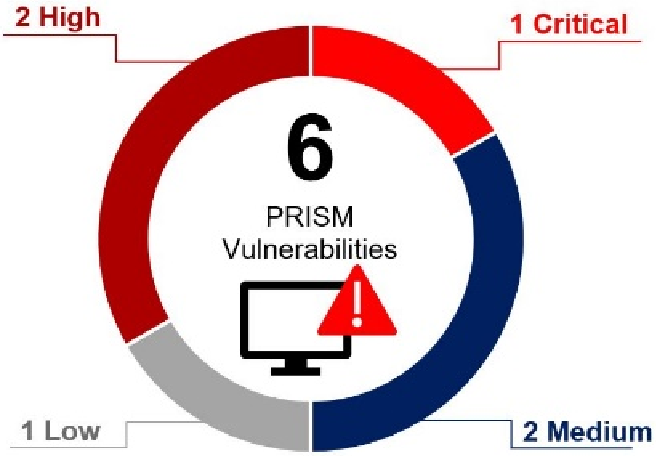
Without confirmation of fulfillment of RBT requirements by IT contractors, the EPA has limited assurance that contractors are maintaining and acquiring the technical skills and knowledge needed to help the EPA maintain a robust information security posture. In addition, if contractors do not comply with Agency guidance on IT training, they could maintain unauthorized access to EPA information systems and data.

OPP Needs to Install Security Updates in a Timely Manner

The OPP did not deploy the Oracle bundle patch on the PRISM production database within the Agency's required time frames. The OPP took eight months to deploy a bundle of PRISM patches that addressed vulnerabilities identified by the National Institute of Standards and Technology's National Vulnerability Database.

Between April 24, 2017, and October 19, 2017, the National Institute of Standards and Technology's National Vulnerability Database identified six vulnerabilities in the version of the PRISM database that the EPA was using. Figure 3 breaks down the six vulnerabilities according to the severity levels.

Figure 3: National Institute of Standards and Technology-identified PRISM vulnerabilities



Source: OIG analysis of the vulnerabilities identified in the National Institute of Standards and Technology's National Vulnerability Database that affect the version of Oracle used by the PRISM production database. (EPA OIG image)

The vendor released a bundle patch addressing the vulnerabilities on July 13, 2018. However, the OPP did not install the bundle patch until March 30, 2019—eight months later. Per EPA policy, the low-priority vulnerabilities should have been patched within 30 days, and the medium- and high- or critical-priority vulnerabilities should have been patched within seven and two days, respectively.

OPP personnel stated that the delay in deploying the bundle patch was related to challenges involving the acquisition of the Oracle Database Appliance from the vendor in 2019, the lengthy Federal Information Technology Acquisition Reform Act review process, and the relocation of the PRISM production servers from the EPA's Potomac Yard location to the EPA's Research Triangle Park location. We found that the OPP lacked management oversight in that it did not prioritize the installation of the bundle patch as required by EPA policies and federal regulations. Without timely deployment of patches to remediate known critical- and high-priority vulnerabilities, the security and integrity of the data within the PRISM database are at risk of being compromised.

Recommendations

We recommend that the assistant administrator for Mission Support:

3. Develop and implement a process to store certifications collected for annual role-based training requirements in a centralized, properly restricted location.

We recommend that the assistant administrator for Chemical Safety and Pollution Prevention:

4. Implement controls to comply with federally and Agency-required time frames to install patches to correct identified vulnerabilities in the Pesticide Registration Information System application.

Agency Response and OIG Assessment

The OMS concurred with Recommendation 3 and completed corrective actions on October 20, 2021. We consider Recommendation 3 completed. The OCSPP concurred with Recommendation 4 and provided acceptable planned corrective actions with estimated milestone dates. We consider Recommendation 4 resolved with corrective actions pending. The OCSPP's response to the draft report is in Appendix B, and the OMS's response to the draft report is in Appendix C.

Status of Recommendations

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date
1	6	Update the Agency's audit tracking system with the correct completion dates and reasons for the delays for corrective actions related to Recommendation 4 of EPA OIG Report Number 19-P-0195, *Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement*, issued June 21, 2019, as required by EPA Manual 2750, *Audit Management Procedures*.	C	Assistant Administrator for Chemical Safety and Pollution Prevention	9/29/21
2	7	Instruct program managers that they must validate that corrective actions are completed before closing them in the Agency's audit tracking system.	R	Assistant Administrator for Chemical Safety and Pollution Prevention	12/31/21
3	11	Develop and implement a process to store certifications collected for annual role-based training requirements in a centralized, properly restricted location.	C	Assistant Administrator for Mission Support	10/20/21
4	11	Implement controls to comply with federally and Agency-required time frames to install patches to correct identified vulnerabilities in the Pesticide Registration Information System application.	R	Assistant Administrator for Chemical Safety and Pollution Prevention	10/31/23

[1] C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

List of Recommendations Selected for Detailed Review

OIG report number, title, and issuance date	Recommendation	Agency agreed-to corrective action(s)	Estimated completion date
17-P-0029, *Acquisition Certifications Needed for Managers Overseeing Development of EPA's Electronic Manifest System*, 11/7/16	We recommend that the assistant administrator for Land and Emergency Management: 2. Implement internal controls to enforce the requirement that the e-Manifest system program and project managers obtain the Federal Acquisition Certification for Program and Project Managers – Information Technology specialized certification once the agency issues the new EPA Federal Acquisition Certification for Program and Project Managers program guidance.	ORCR will amend the position descriptions of personnel covered by the OIG's recommendation to reflect the requirement for the Federal Acquisition Certification for Program and Project Managers – Information Technology. In addition, ORCR will add this requirement as a performance measure to the Performance Appraisal and Recognition System Performance Standards of covered personnel. This will allow ORCR to conduct a midyear and yearly evaluation of compliance with the certification requirements of the guidance. ORCR commits to add this requirement to pertinent performance agreements that will be put in place for FY 2017. Lastly, ORCR will submit revised position descriptions for covered personnel to OARM by December 2016.	12/30/16
17-P-0344, *EPA Lacks Processes to Validate Whether Contractors Receive Specialized Role-Based Training for Network and Data Protection*, 7/31/17	We recommend that the assistant administrator for Administration and Resources Management: 1. Update the EPA Acquisition Guide to include cybersecurity tasks contained in Interim Policy Notice # 17-01, *Use of 22 Cybersecurity Tasks* (December 2016).	OAM does not feel comfortable setting any date for this Interim Policy Notice (IPN) # 17- 01 – Use of 22 Cybersecurity Tasks (December 2016), because this is really an OMB initiative. EPA, in being proactive, developed/prepared the IPN as official agency acquisition policy to be followed. With that said, an estimated milestone date would be October 31, 2019. This is contingent upon the: 1) use of the tasks in solicitations and the receipt of comments/feedback from the vendor communities; and/or 2) OMB's release of cybersecurity clauses via FAR (FAC-xx).	10/31/19

OIG report number, title, and issuance date	Recommendation	Agency agreed-to corrective action(s)	Estimated completion date
	We recommend that the assistant administrator for Environmental Information and the chief information officer: 3. Work with the Assistant Administrator for Administration and Resources Management to implement a process that requires appropriate agency personnel to maintain a listing of contractor personnel who have significant information security responsibilities and are required to take role-based training. This process should require appropriate agency personnel to validate and report to the Chief Information Security Officer that all relevant contractor personnel have completed role-based training.	OEI agrees with the revised recommendation, with a few clarifications. First, we would ask that the recommendation be changed from “Implement a process” to state that “OEI will work with the Assistant Administrator for Administration and Resources Management to implement a process.” This may require actions from Contracting Officer Representatives and would necessitate coordination with OARM. Second, OEI would attest that Agency personnel should respond to the Chief Information Security Officer, not the SAISO, that all relevant contractor personnel have completed role-based training.	12/31/18
	4. Include the number of contractors who have significant information security responsibilities and have completed the required role-based training in the Chief Information Officer’s Annual Federal Information Security Modernization Act reports submitted to the Office of Management and Budget.	OEI agrees in part that based upon a recent change in A-130, Appendix I, this requirement can be met by the end of FY 17.	9/30/17
18-P-0298, *Management Alert: EPA’s Incident Tracking System Lacks Required Controls to Protect Personal Information*, 9/28/18	We recommend that the Assistant Administrator for Environmental Information: 1. Develop and implement a strategy that protects the confidentiality of personally identifiable information and sensitive personally identifiable information, as required by federal and EPA privacy and password guidance, for incident tickets in the current incident tracking system.	Implement a strategy to redact PII and SPII in incident tickets, and disconnect the current incident tracking system from the network by September 30, 2018.	12/31/19
	2. Update standard operating procedures for EPA incident tracking system help desk technicians. Establish controls for technicians to comply with federal personally identifiable information requirements when they handle incident tickets that require them to collect personally identifiable information and sensitive personally identifiable information.	EPA management indicated that standard operating procedures were updated on July 31, 2018 and they provided a copy of the updated procedures.	7/31/18
	3. Complete a System of Records Notice for the replacement incident tracking system.	A new System of Records Notice for the replacement incident tracking system will be completed at the end of Q3 FY19	6/30/19

OIG report number, title, and issuance date	Recommendation	Agency agreed-to corrective action(s)	Estimated completion date
	4. Update the EPA's system security plan, privacy impact assessment and other necessary security documentation to specify that the replacement system will contain personally identifiable information and sensitive personally identifiable information.	System security plan (SSP), privacy impact assessment (PIA) and other necessary documentation for SNOW and Remedy will be updated to reflect what is in the recommendation.	12/31/20*
19-P-0158, *Insufficient Practices for Managing Known Security Weaknesses and System Settings Weaken EPA's Ability to Combat Cyber Threats*, 5/21/19	We recommend that the assistant administrator for Mission Support: 2. Establish a process to periodically review the agency's information security weakness tracking system's settings to validate that each setting is appropriately implemented and compliant with the agency's standards.	The EPA concurs with the recommendation and will establish a process to periodically review settings in the agency's information security weakness tracking system to validate that each setting is appropriately implemented and compliant with the agency's standards	10/31/20
	3. Collaborate with the vendor of the agency's information security weakness tracking system to determine whether audit logging to capture "all data changes" is an available security feature within the agency's information security weakness tracking system and, if so, activate the audit log settings to capture all data changes. If audit logging is not available, establish compensating controls within the agency's information security weakness tracking system that would record or describe what data has been changed.	The EPA concurs with the first part of the recommendation and will continue to collaborate with the vendor to determine whether audit logging to capture "all data changes" is an available security feature within the agency's information security weakness tracking system and, if so, activate the audit log settings to capture all data changes.	10/31/20
		The EPA partially concurs with the second part of the recommendation. Given that the audit log function built into an application is the control within that application to record changes, it is unlikely compensating controls will be available within the tool. However, the EPA will review possibilities and implement what can be reasonably accomplished within the tool.	11/30/20

OIG report number, title, and issuance date	Recommendation	Agency agreed-to corrective action(s)	Estimated completion date
19-P-0195, *Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement*, 6/21/19	We recommend that the Assistant Administrator for Chemical Safety and Pollution Prevention: 2. Complete the actions and milestones identified in the Office of Pesticide Programs' PRIA Maintenance Fee Risk Assessment document and associated plan regarding the fee payment and refund posting processes.	OPP will research the feasibility of utilizing an automated solution for posting fee payments and fee refunds. As a first step, OPP will investigate the possibility of utilizing the Pesticide Submission Portal (PSP) to allow the Registrants to submit fee payments. By October 2019, a document of findings will be presented to the OPP senior leadership team for consideration.	12/31/20*
	4. Implement controls to comply with federally required time frames to install patches to correct identified vulnerabilities in the Pesticide Registration Information System.	Currently, EPA's Office of Mission Support (OMS) manages the automated patch management systems called Continuous Diagnostics Monitoring and Big Fix to determine patches and the state of information system components with regards to flaw remediation (i.e., software patching) in accordance with (IAW) NIST SP 800-53r4 SI-2(1), SI-2(2). OPP will comply with OMS guidance for federally required time frames to install patches to correct identified vulnerabilities in PRISM and the OPP LAN. By October 2019, OPP will update its PRISM and OPP LAN System Security Plan to reflect these procedures.	10/31/19
	5. Implement the EPA's patch management process for the Pesticide Registration Information System.		
20-P-0007, *Management Alert: EPA Still Unable to Validate that Contractors Received Role-Based Training for Information Security Protection*, 10/21/19	We recommend that the assistant administrator for Mission Support: 3. Implement a plan to analyze the EPA's information technology services contractual agreements initiated prior to *EPA Acquisition Guide* 39.1.2 to (a) determine how many of these agreements require modification to include role-based training requirements and (b) include the training requirements in the respective agreements.	OMS will issue a memorandum to the Senior Resource Officials (SROs), Junior Resource Officials (JROs), OAS Division Directors, and Regional Acquisition Managers by January 28, 2020, requiring contracting officers in concert with program CORs and OMS/EI representatives, to review and analyze active information technology services contractual agreements, and ascertain that role-based training requirement is included when contractual agreements require EPA contractors to perform work that has significant information security responsibilities. Where language is discovered to be absent, contracting officers will modify the contracts to include the RBT requirement language. OMS will request that SROs certify completion of the review, analysis, and inclusion of RBT requirement language in IT contracts under their cognizance.	4/10/20

Report number, name, and date	Recommendation	Agency agreed-to corrective action(s)	Estimated completion date
20-E-0309, *EPA Needs to Improve Processes for Securing Region 8's Local Area* Network, 9/10/20	We recommend that the chief financial officer: 6. Coordinate with regions to implement internal controls to determine whether personally identifiable information is protected on regional Superfund Cost Recovery Package Imaging and Online System servers.	OCFO/OTS will coordinate with EPA Regions to implement a Memorandum of Understanding. The intent is for the MOU to require each Regional Senior Information Official to certify that PII on regional SCORPIOS servers is protected in accordance with EPA's IT Security policies. Estimated timing to complete the documents is October 30, 2020. In addition to the MOU with each of the EPA Regions, the OCFO has identified nearly 20,000 PII records that may be appropriate for removal from the regional databases. The OCFO will work with regional contacts to verify and delete the records which will further reduce risk of PII disclosure.	10/30/20

Source: OIG analysis of audit reports and all subsequent Agency responses to those reports, which are published on the OIG internet. (EPA OIG table)

* Estimated completion date was extended beyond our fieldwork time frame.

Legend:

CISO	Chief Information Security Officer	OPP	Office of Pesticide Programs
COR	Contracting Officer Representative	ORCR	Office of Resource Conservation and Recovery
FAC	Federal Advisory Committee	OTS	Office of Technology Solutions
FAR	Federal Acquisition Regulation	PIA	Privacy Impact Assessment
IPN	Interim Policy Notice	PII	Personally Identifiable Information
IT	Information Technology	PRIA	Pesticide Registration Improvement Act
JRO	Junior Resource Official	PSP	Pesticide Submission Portal
LAN	Local Area Network	Q3	Third Quarter
MOU	Memorandum of Understanding	SAISO	Senior Agency Information Security Officer
NIST	National Institute of Standards and Technology	SCORPIOS	Superfund Cost Recovery Package Imaging and Online System
OAM	Office of Acquisition Management	SNOW	ServiceNow
OARM	Office of Administration and Resources Management	SPII	Sensitive Personally Identifiable Information
OCFO	Office of the Chief Financial Officer	SRO	Senior Resource Official
OEI	Office of Environmental Information	SSP	System Security Plan

Appendix B

OCSPP's Response to Draft Report

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

OFFICE OF CHEMICAL SAFETY
AND POLLUTION PREVENTION

MEMORANDUM

SUBJECT: Response to Draft Report entitled, EPA's Information Technology Audit Follow-Up Processes Lack Management Oversight, Project No. OA-FY21-0067

FROM: Michal Ilana Freedhoff, Ph.D.
Assistant Administrator

MICHAL FREEDHOFF
Digitally signed by MICHAL FREEDHOFF
Date: 2021.10.18 18:09:22 -04'00'

TO: Sean W. O'Donnell
Inspector General

This memorandum responds to the Office of Inspector General's (OIG) Draft Report entitled, EPA's Information Technology Audit Follow-Up Processes Lack Management Oversight, Project No. OA-FY21-0067, September 23, 2021.

I. General Comments:

The Office of Chemical Safety and Pollution Prevention (OCSPP) appreciates the OIG's review and assessment of the Agency's compliance with key internal control requirements (data quality; policies and procedures) related to enhancing information technology security. Specifically, the OIG examined whether:

- The EPA completed corrective actions for agreed-to cybersecurity audit recommendations in OIG reports issued from fiscal years 2017 through 2020.
- The actions taken by the EPA effectively resolved the weaknesses identified in select audit reports.

II. OCSPP's Response to the Recommendations:

Recommendation 1: Update the Agency's audit tracking system with the correct completion dates and reasons for the delays for corrective actions related to Recommendation 4 of Report Number 19-P-0195, as required by EPA Manual 2750.

- **Proposed Corrective Action 1**: On September 29, 2021, the OCSPP Senior Audit Liaison corrected the date of completion for Recommendation 4 from August 14, 2019, to December 31, 2020, in the Agency's EAMS Audit Database. There is no field in EAMS for adding a "reason for delay."

- **Target Completion Date**: Completed September 29, 2021.

Recommendation 2: Instruct program managers that they must validate that corrective actions are completed before closing them in the Agency's audit tracking system.

- **Discussion**: In 2019, OCSPP's normal business practice was for the responsible manager to validate the completion of a corrective action by communicating via email to the Audit Liaison and by attaching appropriate supporting documentation as proof of completion. As the Draft Report notes, this was the process followed in this case, but the responsible manager erroneously concluded that the required updates were completed on August 14, 2019.

  OCSPP's current business practice adds an additional layer of management review to the process that was used in 2019. The responsible manager now prepares a formal memo to the Office Director, stating what actions were completed and attaching supporting documentation as proof of completion. The Office Director reviews the memo and documentation, and if he/she agrees it is sufficient, signs the document and transmits it to the Audit Liaison.

- **Proposed Corrective Action 2**: The current OCSPP business practice, which requires a formal memo to the Office Director, followed by Office Director review and signature, adds a layer of substantive review and management accountability to the previous process for declaring a corrective action to be completed. To ensure that all managers understand the importance of this process, the OCSPP Senior Audit Liaison will send a memo to all OCSPP managers outlining their duties and responsibilities.

- **Target Completion Date**: December 31, 2021.

Recommendation 3: Develop and implement a process to store certifications collected for annual role-based training requirements in a centralized, properly restricted location.

- The Office of Mission Support is submitting a separate response that will address this recommendation.

Recommendation 4: Implement controls to comply with federal and Agency required timeframes to install patches to correct identified vulnerabilities in the Pesticide Registration Information System application.

- **Discussion**: OCSPP agrees with the OIG's recommendations to implement controls to comply with federal and Agency required timeframes to install patches to correct identified vulnerabilities in the Pesticide Registration Information System application.

The Pesticide Registration Information System application resides on outdated technology, which prevents OCSPP IT staff from applying current patches to the system since December 2020, without rendering the system inoperable.

Applying current patches to the Pesticide Registration Information System application would result in OCSPP being without the necessary information technology to process statutorily-mandated pesticide registration and re-registration activities.

- **Proposed Corrective Action 4**: On September 30, 2021, OCSPP IT staff submitted a Plan of Action and Milestones (POA&M) into the Agency's XACTA system for review and approval from the Office of Mission Support, Office of the Chief Information Officer.

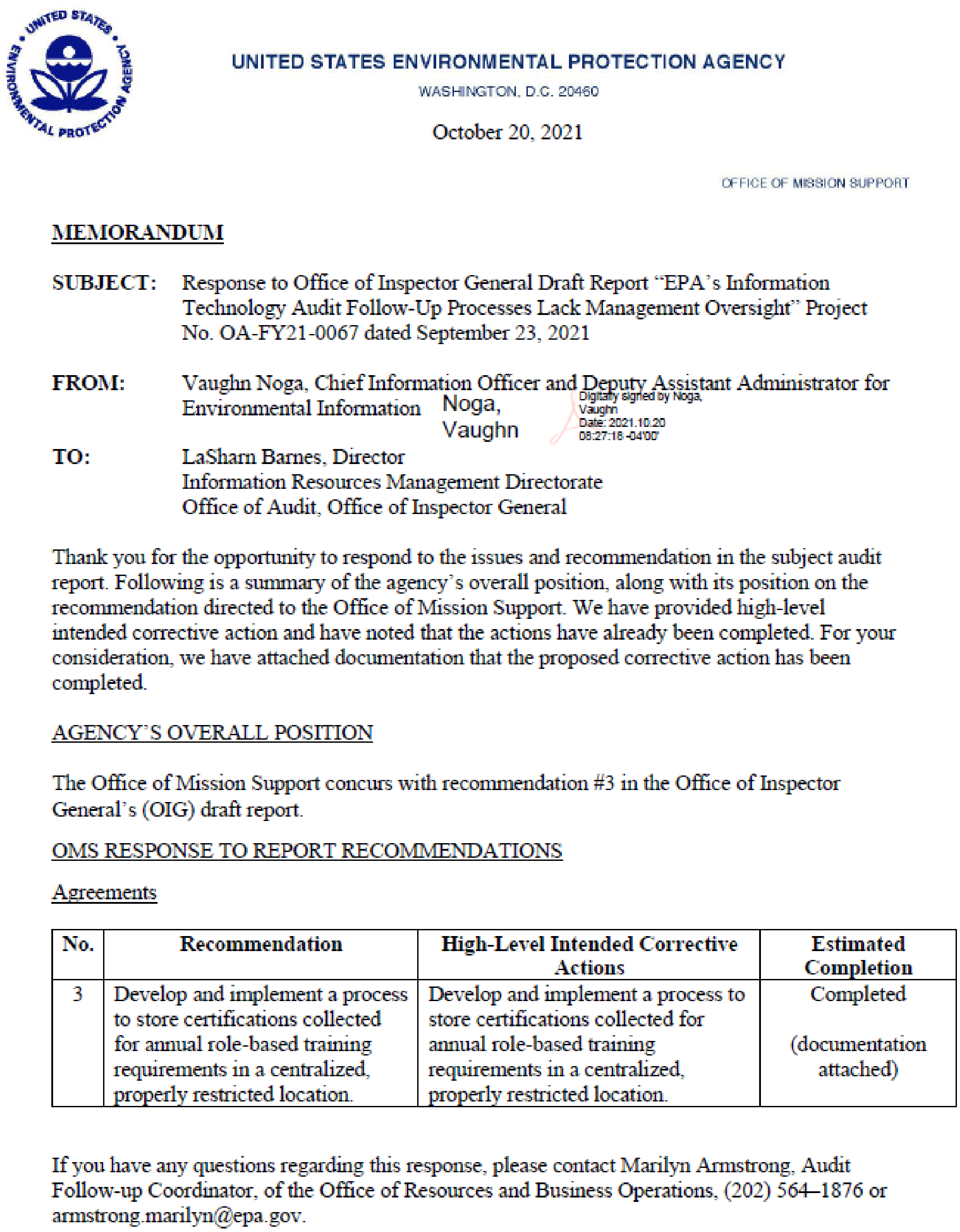
  The POA&M calls for a comprehensive upgrade to the underlying Pesticide Registration Information System application with built-in internal controls to comply with federal and Agency required timeframes to install patches to correct identified vulnerabilities. OCSPP anticipates that this comprehensive upgrade should be in place by October 31, 2023.

- **Target Completion Date**: October 31, 2023.

Cc: OCSPP DAAs
OPP OD, DOD
Hayley Hughes, OPS OD
Delores Barber, OPS ITRMD
Hamaad Syed, OPS ITRMD
LaSharn Barnes, OIG Office of Audit
LaVonda Harris-Claggett, OIG Office of Audit
Eric Jackson, Jr., OIG Office of Audit
Alonzo Munyeneh, OIG Office of Audit
Jeremy Sigel, OIG Office of Audit
Sabrena Stewart, OIG Office of Audit
Janet L. Weiner, OCSPP Senior Audit Liaison
Cameo Smoot, OPS Office Audit Liaison

Appendix C

OMS's Response to Draft Report



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

October 20, 2021

OFFICE OF MISSION SUPPORT

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report "EPA's Information Technology Audit Follow-Up Processes Lack Management Oversight" Project No. OA-FY21-0067 dated September 23, 2021

FROM: Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Environmental Information

Noga, Vaughn

Digitally signed by Noga, Vaughn
Date: 2021.10.20 08:27:18 -04'00'

TO: LaSharn Barnes, Director
Information Resources Management Directorate
Office of Audit, Office of Inspector General

Thank you for the opportunity to respond to the issues and recommendation in the subject audit report. Following is a summary of the agency's overall position, along with its position on the recommendation directed to the Office of Mission Support. We have provided high-level intended corrective action and have noted that the actions have already been completed. For your consideration, we have attached documentation that the proposed corrective action has been completed.

AGENCY'S OVERALL POSITION

The Office of Mission Support concurs with recommendation #3 in the Office of Inspector General's (OIG) draft report.

OMS RESPONSE TO REPORT RECOMMENDATIONS

Agreements

No.	Recommendation	High-Level Intended Corrective Actions	Estimated Completion
3	Develop and implement a process to store certifications collected for annual role-based training requirements in a centralized, properly restricted location.	Develop and implement a process to store certifications collected for annual role-based training requirements in a centralized, properly restricted location.	Completed (documentation attached)

If you have any questions regarding this response, please contact Marilyn Armstrong, Audit Follow-up Coordinator, of the Office of Resources and Business Operations, (202) 564–1876 or armstrong.marilyn@epa.gov.

Attachments:
RBT Attestation Procedure - October 2021
RBT SharePoint Folder Screenshot - October 2021

Cc: Jeremy Sigel
La Vonda Harris-Claggett
Alonzo Munyeneh
Eric Jackson
James Hatfield
Erin Collard
Austin Henderson
David Alvarado
Tonya Manning
Lee Kelly
Kathryn Peele
James Hunt
Dan Coogan
Jan Jablonski
Monisha Harris
Marilyn Armstrong
Andrew LeBlanc
Jose Kercado

Distribution

The Administrator
Deputy Administrator
Chief of Staff, Office of the Administrator
Deputy Chief of Staff, Office of the Administrator
Agency Follow-Up Official (the CFO)
Assistant Administrator for Chemical Safety and Pollution Prevention
Assistant Administrator for Mission Support
Principal Deputy Assistant Administrator for Mission Support
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Deputy Assistant Administrator for Chemical Safety and Pollution Prevention
Deputy Assistant Administrator for Management, Office of Chemical Safety and Pollution Prevention
Deputy Assistant Administrator for Mission Support
Director, Office of Continuous Improvement, Office of the Chief Financial Officer
Director, Office of Pesticide Programs, Office of Chemical Safety and Pollution Prevention
Director, Office of Resources and Business Operations, Office of Mission Support
Audit Follow-Up Coordinator, Office of the Administrator
Senior Audit Advisor, Office of Chemical Safety and Pollution Prevention
Audit Follow-Up Coordinator, Office of Mission Support
Audit Liaison, Office of Pesticide Programs, Office of Chemical Safety and Pollution Prevention