U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Ensuring the safety of chemicals
Operating efficiently and effectively

Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement

Report No. 19-P-0195 **June 21, 2019**

Report Contributors:

Rudolph M. Brevard
Harry Lamptey
Alonzo Munyeneh
Teresa Richardson
Gina Ross
Albert E. Schmidt

Abbreviations

CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
FIFRA	Federal Insecticide, Fungicide, and Rodenticide Act
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPP	Office of Pesticide Programs
POA&M	Plan of Action and Milestones
PRIA	Pesticide Registration Improvement Act
PRISM	Pesticide Registration Information System

Cover Image: The EPA's FIFRA and PRIA systems have internal control deficiencies relating to the fee registration process, system vulnerability mitigation and database security. (EPA OIG image)

Disclaimer: Any product names used in this report are for illustrative purposes only and do not constitute an endorsement of any products.

Are you aware of fraud, waste or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, DC 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our OIG Hotline.

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

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

U.S. Environmental Protection Agency
Office of Inspector General

19-P-0195
June 21, 2019

At a Glance

Why We Did This Project

The Office of Inspector General (OIG) conducted this audit of the information technology security controls for the U.S. Environmental Protection Agency (EPA) systems and servers hosting Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) and Pesticide Registration Improvement Act (PRIA) data. Our audit objectives specifically addressed controls relating to registration fees, the testing and correction of system vulnerabilities, and database security.

Under FIFRA, as amended by PRIA, the EPA regulates the distribution, sale and use of all pesticides in the United States and establishes maximum allowable levels of pesticide residues in food, thereby safeguarding the nation's food supply.

This report addresses the following:

- *Ensuring the safety of chemicals.*
- *Operating efficiently and effectively.*

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

List of OIG reports.

Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement

What We Found

Proper vulnerability testing, fee registration and database controls are essential to the security of the EPA's FIFRA and PRIA systems.

The EPA has adequate controls over the posting of FIFRA and PRIA financial transactions into the agency's accounting system (Compass Financials). However, the EPA's FIFRA and PRIA systems have internal control deficiencies relating to the fee registration process, system vulnerability mitigation and database security. We tested controls in these areas to verify their compliance with federal standards and guidance, as well as with EPA policies and procedures. We noted the following conditions:

- There were inconsistencies and errors related to transactions in the FIFRA and PRIA fee data posted between the Office of Pesticide Programs' pesticide registration system and Compass Financials.
- Twenty of the 29 high-level vulnerabilities identified by the agency in 2015 and 2016 remained uncorrected after the allotted remediation time frame. In addition, we tested 10 of the 20 uncorrected vulnerabilities and found that required plans of action and milestones for remediation were not created for any of them.
- The Office of Pesticide Programs needs to improve the security for one of the FIFRA and PRIA databases, including password controls, timely installation of security updates and restriction of administrative privileges.

Recommendations and Planned Agency Corrective Actions

We recommend that the Assistant Administrator for Chemical Safety and Pollution Prevention implement the following:

- Internal controls for the fee posting and refund processes.
- Corrective actions identified in the agency's risk assessment of those processes.
- A formal process for creating plans of action and milestones, and tracking vulnerability mitigation.
- Controls related to database security.

We met with agency representatives about our draft report. The agency agreed with all seven of our recommendations. The agency completed or provided acceptable corrective actions and milestones for all recommendations. The agency completed corrective actions for Recommendations 1, 3, 6 and 7. Recommendations 2, 4 and 5 are resolved with corrective actions pending.

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

OFFICE OF
INSPECTOR GENERAL

June 21, 2019

MEMORANDUM

SUBJECT: Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement
Report No. 19-P-0195

FROM: Charles J. Sheehan, Deputy Inspector General

TO: Alexandra Dapolito Dunn, Assistant Administrator
Office of Chemical Safety and Pollution Prevention

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). The project number for this audit was OA-FY17-0091. 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 three offices with primary responsibilities for the issues discussed in this report are the Office of Pesticide Programs within the Office of Chemical Safety and Pollution Prevention, and the Office of Budget and Office of the Controller, both within the Office of the Chief Financial Officer.

Action Required

In accordance with EPA Manual 2750, your office completed or provided acceptable corrective actions and milestone dates in response to OIG recommendations. All recommendations are resolved, and 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

-- continued --

Appendices

Chapter 1
Introduction

Purpose

The U.S. Environmental Protection Agency's (EPA's) Office of Inspector General (OIG) conducted this audit to accomplish the following objectives:

- Determine whether the vulnerability testing of servers that host and manage Pesticide Registration Improvement Act (PRIA) and Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) applications is complete, and whether the agency is taking actions to correct identified vulnerabilities.
- Determine whether controls exist to verify the completeness of registrations processed within the PRIA and FIFRA systems, and whether fees are recorded in the EPA's Compass Financials.
- Review the information technology security of the database containing PRIA and FIFRA information.

Compass Financials is a web application that the EPA uses to manage, budget and track expenditures and to support the financial management information requirements of managers and administrative staff.

Background

Under FIFRA, as amended by PRIA, the EPA regulates the distribution, sale and use of all pesticides in the United States and establishes maximum allowable levels of pesticide residues in food, thereby safeguarding the nation's food supply. The EPA's Office of Pesticide Programs (OPP), within the Office of Chemical Safety and Pollution Prevention (OCSPP), implements the FIFRA program, including the elements of the program added by PRIA.

FIFRA and PRIA Overview

Congress amended FIFRA in 1988 to impose a one-time reregistration fee for older pesticides and an annual maintenance fee for each pesticide registration.[1] These fees are deposited into the U.S. Department of the Treasury's Reregistration and Expedited Processing Fund.

PRIA, first enacted in 2003, amended FIFRA to establish a new system for registering pesticides.[2] PRIA prescribes the fee amounts and decision review

[1] FIFRA § 4, Public Law 100-532 § 102(a), October 25, 1988.
[2] FIFRA § 33.

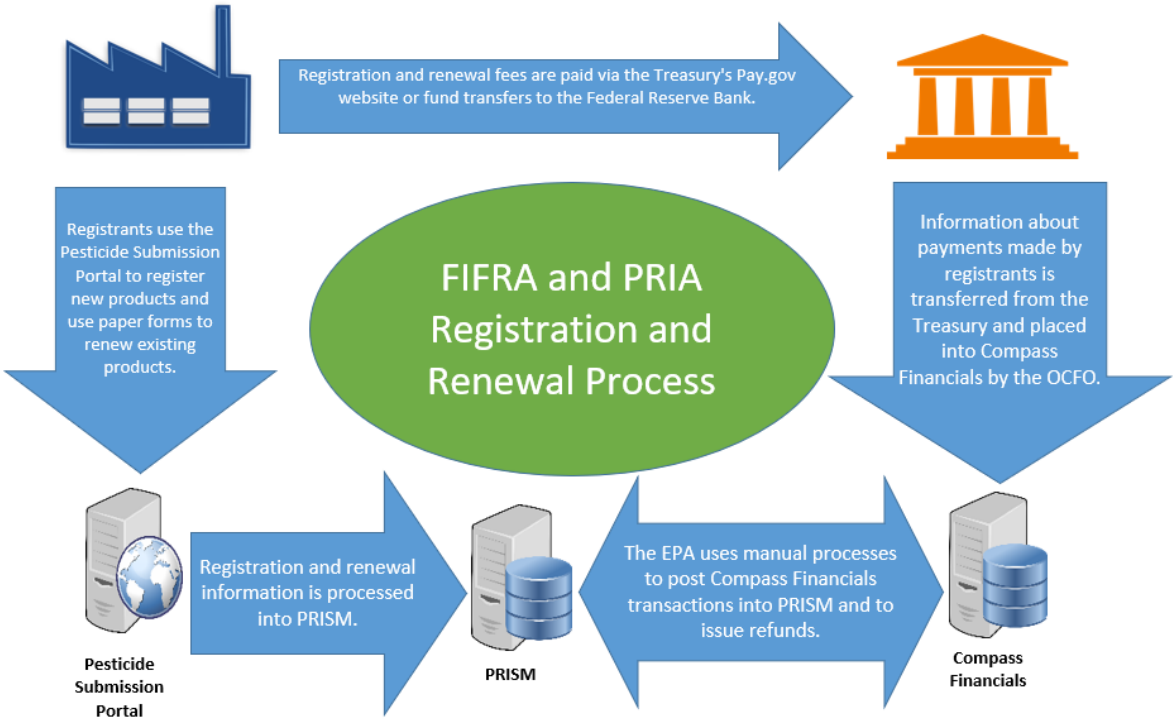
times for each type of registration action. These fees are deposited into the Department of the Treasury's Pesticide Registration Fund.

Registration and Maintenance Fee Process

To register new pesticide products, companies submit their PRIA registrations to the EPA by entering them into the EPA's Pesticide Submission Portal. This registration information is then processed into the EPA's Pesticide Registration Information System (PRISM). To renew registrations, companies mail a paper Pesticide Registration Maintenance Fee Filing Form to the EPA.

Registrants pay PRIA registration and FIFRA maintenance fees via either the Department of the Treasury's Pay.gov website or fund transfers to the Federal Reserve Bank. The Department of the Treasury informs the EPA of the payments made, and fee payment records are loaded into Compass Financials by the EPA's Office of the Chief Financial Officer (OCFO). The OPP then relies on manual processes to verify the collection of fee payments for registrations and annual maintenance. An OPP processing official uses the agency's Yearly Maintenance System—a standalone database—to manipulate Compass Financials information into files that can be entered into PRISM, which then triggers the OPP to process registrations and maintenance fee submissions. The processing official also uses manual processes to identify overpayments and possible refunds. For example, the EPA can issue refunds if a registrant overpays. Figure 1 provides an overview of the FIFRA and PRIA registration and maintenance fee process.

Figure 1: FIFRA and PRIA registration and maintenance fee process



Source: OIG image.

Responsible Offices

Three offices have primary responsibility for the audit issues discussed: the OCSPP's OPP, the OCFO's Office of Budget and the OCFO's Office of the Controller.

Scope and Methodology

We performed this performance audit from January 2017 through March 2019 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 believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We evaluated the processes used by the EPA to mitigate vulnerabilities and verify the security of the FIFRA and PRIA databases. We evaluated the timeliness of vulnerability remediation by reviewing whether the vulnerability testing results from calendar years 2015 and 2016 complied with the Chief Information Officer's (CIO's) *Information Security – Risk Assessment Procedures*. We validated the completeness of the vulnerability scans. We relied on the counts and severity of the vulnerabilities identified in the provided reports and did not perform additional test work to verify the accuracy of the reports. The vulnerability testing results were summarized using data analysis software.

To test whether controls exist to verify the completeness of registrations processed, we performed the following actions:

- Examined audit work conducted during the fiscal year 2017 consolidated financial statement audit to determine whether the EPA has a process in place to verify the complete transfer of financial transactions from other financial systems into Compass Financials. This process governs how the EPA transfers FIFRA and PRIA financial transactions from the Department of the Treasury, as well as payroll, contract and grant transactions processed by other EPA or contractor systems. The fiscal year 2017 audit found that the EPA has a process that operates as intended.

- Looked at testing conducted during the fiscal year 2016 FIFRA and PRIA financial statement audit regarding the accuracy of the processing of FIFRA and PRIA collection transactions. These tests identified no exceptions to the recording of fees in Compass Financials.

- Conducted automated data matching to compare the FIFRA and PRIA financial transactions in Compass Financials to those in PRISM. We completed a procedural review of the records of registration and

maintenance fees collected from registrants that were posted in both Compass Financials and PRISM.

- Interviewed OPP personnel in Washington, D.C.

- Tested a judgmental selection of fiscal year 2016 FIFRA and PRIA transactions to verify that transactions posted to Compass Financials appeared in PRISM. We did not test the collection records that were recorded in Compass Financials but not recorded in PRISM; the EPA had finished processing these records only in Compass Financials—and not in PRISM—when we completed that portion of our fieldwork.

- Evaluated PRISM database parameters and user privileges to determine whether they complied with National Institute of Standards and Technology (NIST) 800-53 security controls.[3]

[3] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations,* Special Publication 800-53, April 2013.

Chapter 2
OPP Needs to Improve Internal Controls over FIFRA and PRIA Fee Posting and Refund Processes

While we found that the EPA has adequate controls over the posting of FIFRA and PRIA financial transactions into Compass Financials, the OPP lacks internal controls to prevent errors and data inconsistencies when manually processing and posting FIFRA and PRIA pesticide registration fee information from Compass Financials into PRISM. In addition, oversight over the FIFRA and PRIA refund process needs improvement. Guidance from the Office of Management and Budget (OMB) and the Government Accountability Office specifies that it is management's responsibility to establish internal and transactional controls. However, a single EPA processing official is responsible for extracting the FIFRA and PRIA fee information from Compass Financials and manually posting the information into PRISM. That same official manually initiates the refund process. We noted that the FIFRA and PRIA fee data posted to PRISM did not always match the related transactions in Compass Financials. If entered correctly, FIFRA and PRIA fee payment records in PRISM and Compass Financials should match. The lack of internal controls over the FIFRA and PRIA fee posting and refund processes could result in errors in fee payment and refund data in PRISM.

Federal Guidance Describes Internal Control Responsibilities

In OMB Circular No. A-123,[4] Section III, "Establishing and Operating An Effective System of Internal Control," provides that:

> Management's responsibility is to develop and maintain effective internal control that is consistent with its established risk appetite and risk tolerance levels. In addition, management is responsible for establishing and integrating internal control into its operations in a risk-based and cost beneficial manner, in order to provide reasonable assurance that the entity's internal control over operations, reporting, and compliance is operating effectively.

In addition, the Government Accountability Office's *Standards for Internal Control in the Federal Government* provides that:[5]

> Transaction control activities are actions built directly into operational processes to support the entity in achieving its

[4] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016. Transmitted by OMB Memorandum M-16-17.
[5] Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 10, 2014.

objectives and addressing related risks. "Transactions" tends to be associated with financial processes (e.g., payables transactions), while "activities" is more generally applied to operational or compliance processes. For the purposes of this standard, "transactions" covers both definitions. Management may design a variety of transaction control activities for operational processes, which may include verifications, reconciliations, authorizations and approvals, physical control activities, and supervisory control activities.

Oversight of FIFRA and PRIA Refund Process Needs Improvement

According to the OPP's processing official, there is no review of or oversight over the full refund process. The agency's refund process begins when the EPA processing official receives a request for a refund from the company producing a pesticide. The processing official then performs the following steps:

1. Notifies the OPP pesticide division of the refund transaction request.
2. Uploads the refund information into PRISM using manual extracts from Compass Financials.
3. Prepares a memorandum for supervisory signature acknowledging the request for and issuance of the refund.
4. Manually prepares a packet of supporting documents, including copies and screenshots of the actions taken to process the request.
5. Sends the packet and the signed memorandum to the OCFO, which processes the refund in Compass Financials.

The EPA processing official indicated that there are times when the OCFO rejects refund transactions because of incorrect vendor information and sends the request back to the processing official to verify or correct this information. However, there are no internal controls to confirm that the corrected refund requests returned to the OCFO are properly authorized. When asked about oversight of the fee refund process, the processing official's immediate supervisor said that, beyond signing the letters sent to the OCFO for initial processing, there is no supervisory review of the full refund process.

FIFRA and PRIA Transactions in PRISM and Compass Financials Are Not Always Consistent

FIFRA Fee Payment Transactions

In fiscal year 2016, there were 160 FIFRA fee payment transactions (out of a total of 1,634) in Compass Financials that could not be matched to PRISM using automated processes. Of these 160 unmatched transactions in Compass Financials, we judgmentally selected 15 transactions that ranged from $200 to $184,800.

Our analysis of these 15 FIFRA transactions revealed the following conditions, which are also depicted in Figure 2:

- Nine transactions existed in both PRISM and Compass Financials, but they could not be matched via automated methods due to data inconsistencies between the two systems. We were able to match these transactions using manual processes.

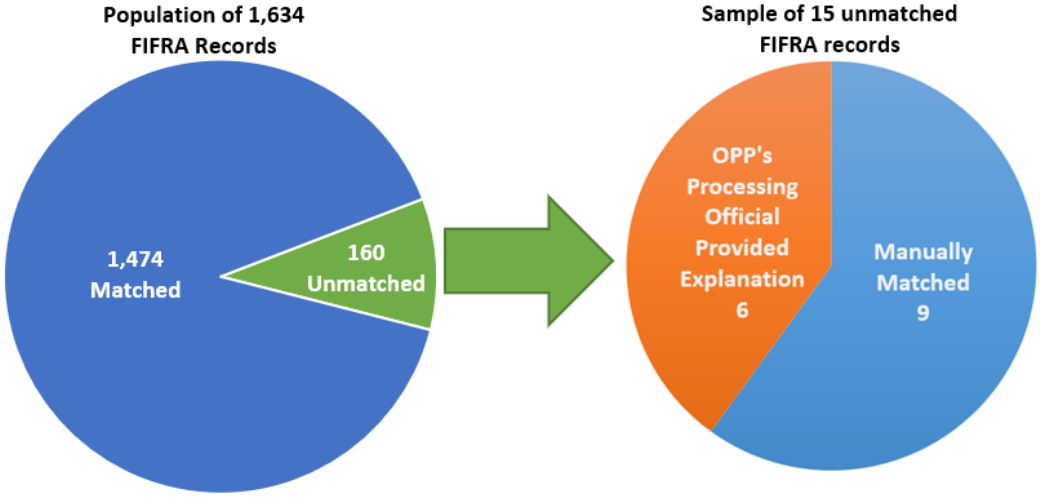
- Six transactions could not be matched via automated methods and could not be manually matched without the assistance of the processing official:

    - Three transactions related to FIFRA fee payments had been refunded because they were accidentally paid twice by a registrant. The overpayments and refunds were not captured in PRISM.

    - Two transactions pertained to an Intra-Governmental Payment and Collection[6] made by another federal agency and had been refunded back to the agency. These refunds were not captured in PRISM.

    - One transaction was a mishandled Intra-Governmental Payment and Collection. This payment was not captured in PRISM.

Figure 2: Summary of FIFRA transactions tested



Source: OIG image.

[6] Per the Bureau of the Fiscal Service website, an Intra-Governmental Payment and Collection "is a way for Federal Program Agencies … to transfer funds from one agency to another."

PRIA Fee Collection Transactions

In fiscal year 2016, there were 404 PRIA fee collection transactions (out of a total of 2,162) in Compass Financials that could not be matched to PRISM using automated processes due to data inconsistencies and timing differences. Of the 404 unmatched transactions in Compass Financials, we judgmentally selected 10 transactions that represented fee transactions of unusual or large dollar amounts.

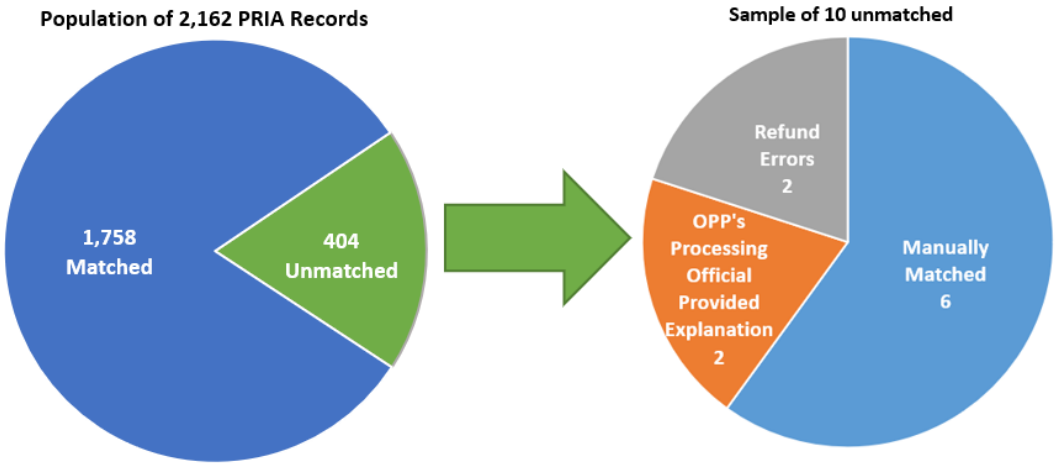
Our analysis of these 10 sampled PRIA transactions revealed the following conditions, which are also depicted in Figure 3:

- Six transactions existed in both PRISM and Compass Financials; however, data inconsistencies prevented automated matches between PRISM and Compass Financials. We were able to match these transactions using manual processes.

- The OPP was able to provide explanations for two unmatched transactions.

- Two transactions were identified as refund posting errors. The OPP provided documentation showing that these two refund errors were corrected.

Figure 3: Summary of PRIA transactions tested



Source: OIG image.

OPP Should Implement Corrective Actions for Fee and Refund Posting Processes

The OPP relies on manual processes for posting fee payments from Compass Financials to PRISM and refunds to Compass Financials. Per Section 1 of OMB Memorandum M-18-23,[7] the OPP should determine if routine processes could be automated to shift resources to high-value activities. Not identifying and implementing possible internal controls over the manual process and not automating the processes with adequate controls could lead to fraudulent refunds and errors in the fee payment and refund data.

In response to our audit, OPP staff developed a *PRIA Maintenance Fee Risk Assessment* document and associated plan that proposed corrective actions and milestones, including:

- Upgrade PRISM to better identify the correct fee for each fee category.
- Hire additional personnel to back up and oversee the fee posting function.
- Hire additional personnel and/or develop a more streamlined information technology system to process registration actions and allow transparency and oversight.
- Modernize the Yearly Maintenance System.

While the risk assessment and associated plan were a positive first step, it is still incumbent upon management to complete the corrective actions identified in the risk assessment, particularly modernizing the Yearly Maintenance System and streamlining/automating routine processes, as feasible, to maintain data integrity.

Recommendations

We recommend that the Assistant Administrator for Chemical Safety and Pollution Prevention:

1. Develop and implement internal controls over the manual processes used to post fee payments from Compass Financials to the Pesticide Registration Information System and post fee refunds from the Pesticide Registration Information System to Compass Financials.
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.

[7] OMB Memorandum M-18-23, *Shifting From Low-Value to High-Value Work*, August 27, 2018.

Agency Response and OIG Evaluation

The OPP agreed with Recommendation 1 and indicated that in April 2019 it developed and implemented internal controls over the manual process used to post fee payments. The Team Leader in the OPP's Information Services Branch is now responsible for reviewing all postings of fee payments from Compass Financials to PRISM, while the Information Services Branch Chief now checks the validity of all fee postings. The corrective action for Recommendation 1 was completed.

Based on our evaluation of Recommendation 2 as it appeared in our draft report and the agency's response to that recommendation, we modified Recommendation 2. We subsequently met with the agency, which agreed with our revised recommendation. The OPP indicated that it is undertaking a modernization effort for its information technology systems, which will enable the OPP to process electronic application and fee submissions through a fully electronic flow environment. This upgrade will be completed in December 2020. Recommendation 2 is resolved with the corrective action pending.

Appendix A contains the agency's full response to our draft report.

Chapter 3
OPP Needs to Strengthen the Process to Remediate Identified Vulnerabilities in a Timely Manner

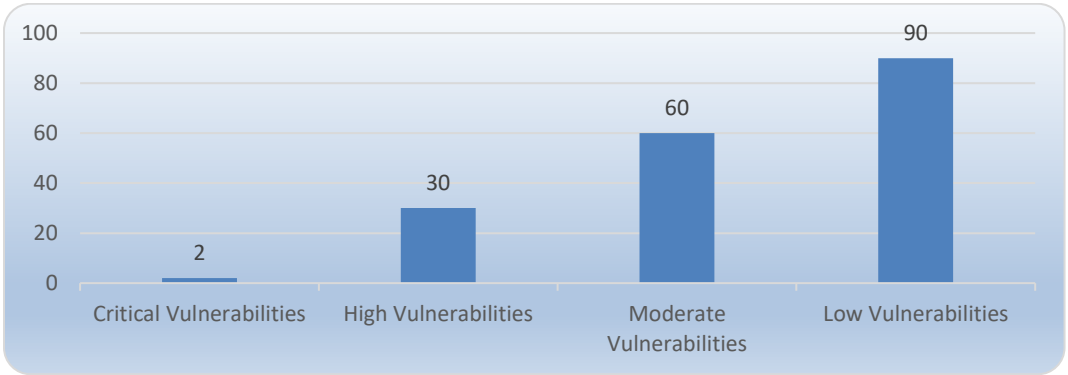
The OPP lacks management controls to remediate identified vulnerabilities in a timely manner. As a result, the vulnerabilities identified during testing of the PRISM servers are not being mitigated within the required time frames. EPA procedures specify the time frames within which EPA offices must remediate critical, high, moderate and low vulnerabilities, as well as the steps these offices must take if the vulnerabilities cannot be remediated within those time frames. However, our analysis showed that the OPP does not have a formal vulnerability mitigation process, nor does it have a formal process for creating plans of action and milestones (POA&Ms) to address vulnerabilities. Without a proper vulnerability mitigation process, the OPP increases its risk of being exploited by threats.

A **POA&M** is a document that identifies tasks to be accomplished to address vulnerabilities. It details the resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

OPP Does Not Remediate Vulnerabilities in a Timely Manner

Identified vulnerabilities are not being remediated as prescribed by EPA procedures. The Office of Mission Support conducts scans of the agency's information systems, including PRISM servers and devices, to identify vulnerabilities. Per the "Vulnerability Scanning" section of the CIO's *Information Security – Risk Assessment Procedures*, system owners shall "[r]emediate legitimate vulnerabilities discovered from scans and penetration testing in accordance with an organizational assessment of risk" and in coordination with agency officials, including the Information Security Officer. Also, this procedure specifies the time frames in which either the vulnerabilities must be remediated or POA&Ms must be created (Figure 4).

Figure 4: Days allotted to mitigate vulnerabilities before a POA&M is required



Source: OIG analysis of the EPA's *Information Security – Risk Assessment Procedures*.

In accordance with the CIO's *Information Security – Risk Assessment Procedures*, the Office of Mission Support provides reports of any identified vulnerabilities to the system owner—in the case of PRISM, the OPP—for remediation. From January 2015 through December 2016, 203 vulnerabilities occurring over 58 PRISM servers and devices were reported to the OPP. Our analysis of the scan results for calendar years 2015 and 2016, however, showed that the OPP is not consistently remediating the identified vulnerabilities within the CIO's required time frames. Table 1 illustrates the days elapsed since the first and last appearances of vulnerabilities within the scan results. For example, we noted that only nine of the 29 high vulnerabilities identified were remediated within 30 days, as required by the CIO's *Information Security – Risk Assessment Procedures*, while one high vulnerability went unresolved for over 360 days.

Table 1: Mitigation of PRISM server vulnerabilities in 2015 and 2016

Days elapsed before vulnerabilities mitigated	Number of vulnerabilities identified for each severity level		
	High	Moderate	Low
1–30	9	60	1
31–60	8	10	3
61–90	4	13	2
91–120	1	31	0
121–150	1	8	0
151–180	3	3	3
181–210	0	4	0
211–240	1	5	0
241–270	0	0	0
271–300	0	0	0
301–330	0	1	0
331–360	1	2	0
>360	1	27	1
Total	**29**	**164**	**10**

Legend: Corrected within the CIO-required time frame
Not corrected within the CIO-required time frame

Source: OIG analysis of EPA data.

In addition, we judgmentally selected 10 of the high-level vulnerabilities identified that exceeded the allotted 30-day remediation period for analysis. There were no POA&Ms in the agency's vulnerability management tracking system for any of these 10 vulnerabilities.

OPP Lacks a Formal Tracking Process to Remediate Vulnerabilities

The OPP has an ad hoc process for mitigating vulnerabilities associated with PRISM, and the office does not consistently follow its formal process for creating

POA&Ms to remediate these vulnerabilities. The EPA, at large, has an official enterprise vulnerability management tracking system that the OPP could use to develop and manage POA&Ms. The EPA notes the vulnerability management tracking system is a Federal Information System Management Act Risk Management Framework agency tool that allows Risk Management Framework documentation and artifacts (e.g., system security plans, vulnerability scans and security assessment reports) to be collected and stored. This tool also allows data related to artifacts (e.g., vulnerability and POA&M information) to be tracked. The vulnerability management tracking system is used to facilitate not only continuous compliance monitoring and system authorization but also continuous management of security compliance, risks, and key elements of the assessment and authorization process for the EPA's information technology systems.

Without implementing a process to track vulnerability mitigation and using the agency's risk management solution, the OPP prolongs its exposure to threats. Specifically, the Office of Mission Support's vulnerability scan reports indicate that the PRISM servers contain vulnerabilities impacting the confidentiality, integrity and availability of FIFRA and PRIA information.

Recommendation

We recommend that the Assistant Administrator for Chemical Safety and Pollution Prevention:

3. Implement a formal process for creating plans of action and milestones in the agency's vulnerability management tracking system to track the mitigation of vulnerabilities identified by the Office of Mission Support.

Agency Response and OIG Evaluation

The OPP agreed with Recommendation 3 and indicated that, as of October 2018, it follows the guidance and formal process issued by the Office of Chemical Safety and Pollution Prevention's Information Systems Security Officer to create POA&Ms and upload artifacts into XACTA. This process allows the OPP to track and mitigate PRISM and other vulnerabilities identified by the Office of Mission Support. Corrective actions for Recommendation 3 were completed.

Appendix A contains the agency's full response to our draft report.

Chapter 4
OPP Needs to Improve Database Controls to Meet Security Requirements

The OPP lacks database controls associated with password management, patch management, and roles and responsibilities for its PRISM database. According to EPA policies, database controls are required to meet federal password guidelines. Additionally, NIST standards require agencies to install relevant system updates and system owners to grant privileges on a need-to-know basis. However, the OPP did not comply with federal or EPA password requirements, did not install patches to mitigate vulnerabilities in accordance with agency information security directives, and did not have controls in place to limit the ability to alter the security settings to only system administrators. Without adequate database controls, the security and integrity of the data within the PRISM database may be compromised.

NIST and EPA Outline System Protection Requirements

NIST and EPA requirements for controls over password strength, patch management, administrative privileges and account management are specified within federal standards and agency procedures. These criteria are outlined in Table 2.

Table 2: NIST and EPA database requirements

Source	Citation	Criteria
Passwords		
NIST	*Security and Privacy Controls for Federal Information Systems and Organizations,* Special Publication 800-53 Rev. 4, April 2013	Agency manages information system passwords by ensuring that passwords have sufficient strength for their intended use and by establishing the maximum lifetime and re-use restrictions.
EPA	*Information Security – Identification and Authentication Procedure*, CIO 2120-P-07.2, November 30, 2015	Passwords for EPA systems must meet the federal requirements defined in Section IA-5 of NIST's *Security and Privacy Controls for Federal Information Systems and Organizations.*
Patch management		
NIST	*Security and Privacy Controls for Federal Information Systems and Organizations*	Per Section SI-2, security-relevant software and firmware updates must be installed within an agency-defined time period of the release.
EPA	*Information Security – Interim System and Information Integrity Procedures,* CIO 2150.3-P-17.1, August 6, 2012	Per Section 6, Part SI-2(k)(i), the agency must promptly install security-relevant software updates, "including patches, services [sic] packs, and hot fixes," per the following timeline: • "Fixes for vulnerabilities ranked high or critical must be tested as soon as possible but no later than two business days. • "Fixes for vulnerabilities ranked moderate to medium must be tested within seven business days. • "Complete testing of fixes for low priority vulnerabilities must be completed within 30 days."

Source	Citation	Criteria
Administrative privileges		
NIST	*Security and Privacy Controls for Federal Information Systems and Organizations*	Per Section AC-6, agencies should implement controls to restrict each user's privilege: "The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."
EPA	*Information Security – Access Control Procedure,* CIO 2150-P-01.2, September 21, 2015	Per Section 6, Part AC-6, system owners and managers should grant privileges on the basis of "least privilege" for moderate and high information systems: "Employ the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) that are necessary to accomplish assigned task in accordance with original organizational missions and functions."
Monitoring administrative access		
NIST	*Security and Privacy Controls for Federal Information Systems and Organization*	Per Section AU-6, the organization reviews and analyzes information system audit records for agency-defined inappropriate or unusual activity and reports any findings to agency-defined personnel or roles. Further, Section AC-5, indicates that agencies need to separate duties to reduce the risk of abuse of authorized privileges and malevolent activity. This guidance includes separating administrative access from individuals who would review the logs of administrative access.
Account management		
NIST	*Security and Privacy Controls for Federal Information Systems and Organizations*	Per Sections AC-2(7), AU-1, AU-2 and AU-6, agencies should implement account management controls for the following actions: • Establishing and administering "privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles." • Monitoring "privileged role assignments." • Taking organization-defined actions "when privileged role assignments are no longer appropriate." • Establishing audit and accountability policies and procedures. • Identifying auditable events. • Reviewing and analyzing "information system audit records."

Source: EPA and NIST.

OPP Needs to Enforce Password Management Policy

Password management controls for the PRISM database did not meet federal or EPA password requirements. Table 3 compares the PRISM password settings with federal and EPA password requirements.

Table 3: PRISM's password settings compared to EPA and NIST password requirements

PRISM password settings	EPA password requirements	NIST password requirements
Passwords must be at least six characters long.	Passwords must be at least 12 characters long.	Information systems enforce complexity based on agency-defined requirements for number of characters.
Passwords must be changed every 90 days.	Passwords must be changed every 60 days.	Information systems enforce password maximum lifetime restrictions.
Passwords may be reused.	Passwords must be changed 24 times before they can be reused, and passwords cannot be reused within 4 years.	Information systems prohibit the re-use of passwords for an agency-defined number of generations.

PRISM password settings	EPA password requirements	NIST password requirements
Passwords must include an uppercase or lowercase alphabetic character and a special or numeric character.	Passwords must contain any three of the following four character types: special, numeric, lowercase alphabetic and uppercase alphabetic.	Information systems enforce complexity based on agency-defined requirements for case sensitivity and a mix of uppercase letters, lowercase letters, numbers and special characters.
Passwords may be similar to older passwords.	When creating new passwords, 50% of the characters in the password must be changed.	Information systems enforce at least an agency-defined number of characters within the password be changed.

Source: OIG analysis of PRISM's password settings, EPA's *Information Security – Identification and Authentication Procedure,* and NIST's *Security and Privacy Controls for Federal Information Systems and Organizations*.

The OPP's information technology managers said that they could not readily change the password settings to meet the requirements; the applicable controls are fixed into a software program and cannot be changed without modifying the program. However, in response to our audit findings, the OPP provided us with copies of configuration changes made to PRISM to comply with the password requirements. On October 5, 2018, OPP changed PRISM's password settings to meet federal and EPA password requirements.

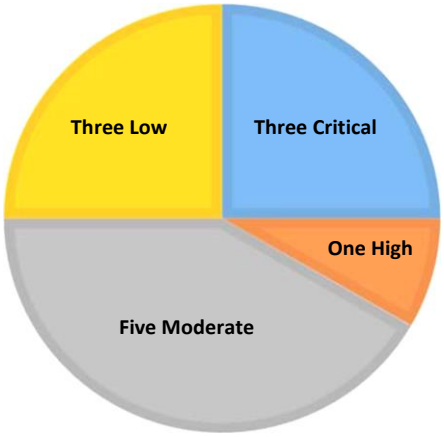
OPP Needs Controls to Install Security Updates in a Timely Manner

The OPP did not always patch the PRISM database within the time frame required by the EPA (identified in the "Patch management" section of Table 2 above). Specifically, in the time period covered by our audit, we found that the OPP took 57 days to deploy a bundle of PRISM patches that addressed vulnerabilities identified by the NIST National Vulnerability Database.

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

Between April 21, 2016, and January 27, 2017, the NIST National Vulnerability Database identified 12 vulnerabilities in the version of the PRISM database being used by the EPA. Figure 5 breaks down these 12 vulnerabilities according to their severity levels. The vendor released a bundle patch addressing these vulnerabilities on December 9, 2016. However, the OPP did not install the bundle patch until February 4, 2017—57 days later. Per EPA policy, the low priority vulnerabilities should have been patched within 30 days, while the high and critical vulnerabilities should have been patched within 2 business days.

Figure 5: NIST-identified PRISM vulnerabilities



Source: OIG image.

When we asked why installing the bundle patch took 57 days, information technology management said that the OPP Local Area Network Manager, who is responsible for overseeing patch installation, was on extended use-or-lose leave. Management also said that the only guidance for patch management comes from the PRISM Control RA-5, *Vulnerability Scanning of the PRISM Security Plan* (Version 3.7). This control, however, focuses on the

mitigation of vulnerabilities after performing scans and is different from vulnerabilities addressed by vendor-supplied patches.

OPP personnel were unable to fulfill their responsibility to oversee patch management in a timely manner, and they did not create or maintain a documented process to consistently apply patches. OPP representatives said that they try to install patches within 2 weeks of release.

OPP Needs to Limit and Adequately Monitor Administrative System Privileges

The OPP did not have controls in place to limit the ability to alter the security settings of other users—including changing their passwords—to only system administrators. We found that this "user security settings" privilege was unnecessarily granted to 35 individuals with active database accounts. Further, the OPP did not perform independent reviews of the use of administrative access to the PRISM database. Although the database is configured to record use of administrative privileges, the OPP indicated that these logs were only reviewed by database administrators, not by independent reviewers.

System administrators said that a development error in PRISM caused the 35 system users to be granted the user security settings privilege. The agency said that it believed access was still restricted, as specialized software is needed to connect to the database. However, information technology security controls should be applied in layers; a single layer should not be relied upon to prevent users from potentially abusing unauthorized access.

Additionally, the OPP did not review the mechanisms by which user privileges were granted when the PRISM database was developed. A system user could take advantage of improper user security settings privileges to gain administrative access to the database by changing the password associated with an administrative user account.

OPP's Ability to Protect PRISM Is Inhibited

The PRISM database is at risk for the unauthorized disclosure and modification of information in the database, as well as possible disruption of service, because the EPA has not implemented the required controls for password strength, patch management, and user and administrative privileges.

Actions Taken by Agency

Prior to the issuance of the draft report, the EPA took corrective actions to bring the PRISM database's password management controls into compliance with federal and EPA password requirements. Further, the EPA indicated that it revoked the administrative privilege of users who do not require that level of access.

Recommendations

We recommend that the Assistant Administrator for Chemical Safety and Pollution Prevention:

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

5. Implement the EPA's patch management process for the Pesticide Registration Information System.

6. Implement periodic review of roles within the Pesticide Registration Information System to determine the appropriateness of privileges assigned to roles and users.

7. Implement procedures for the independent review of administrative access logs for the Pesticide Registration Information System's database.

Agency Response and OIG Evaluation

The OPP agreed with Recommendations 4 and 5 and indicated that by October 2019 it will comply with EPA guidance regarding federally required time frames to install patches to correct identified vulnerabilities. Recommendations 4 and 5 are resolved with corrective actions pending.

The OPP also agreed with Recommendation 6. The OPP said that the Information Security Officer periodically conducts a review of roles and system privileges to ensure that "the appropriate level of access [is] assigned to all users in accordance with the EPA's Chief Information Officer Policy CIO 2150-3." The corrective action for Recommendation 6 was completed as of October 2018.

We met with the OPP regarding Recommendation 7 to discuss the corrective action initially proposed, which we believed did not meet the recommendation's intent. OPP management agreed with our analysis and indicated that the OPP would implement procedures for its Security Officer to independently review administrative access logs for the PRISM database. In a subsequent email, OPP management outlined its revised corrective action plan, which it said was completed in May 2019. We consider corrective action for Recommendation 7 to be completed.

Appendix A contains the agency's full response to our draft report.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Potential Monetary Benefits (in $000s)
1	9	Develop and implement internal controls over the manual processes used to post fee payments from Compass Financials to the Pesticide Registration Information System and post fee refunds from the Pesticide Registration Information System to Compass Financials.	C	Assistant Administrator for Chemical Safety and Pollution Prevention	4/1/19	
2	9	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.	R	Assistant Administrator for Chemical Safety and Pollution Prevention	12/31/20	
3	13	Implement a formal process for creating plans of action and milestones in the agency's vulnerability management tracking system to track the mitigation of vulnerabilities identified by the Office of Mission Support.	C	Assistant Administrator for Chemical Safety and Pollution Prevention	10/31/18	
4	18	Implement controls to comply with federally required time frames to install patches to correct identified vulnerabilities in the Pesticide Registration Information System.	R	Assistant Administrator for Chemical Safety and Pollution Prevention	10/31/19	
5	18	Implement the EPA's patch management process for the Pesticide Registration Information System.	R	Assistant Administrator for Chemical Safety and Pollution Prevention	10/31/19	
6	18	Implement periodic review of roles within the Pesticide Registration Information System to determine the appropriateness of privileges assigned to roles and users.	C	Assistant Administrator for Chemical Safety and Pollution Prevention	10/31/18	
7	18	Implement procedures for the independent review of administrative access logs for the Pesticide Registration Information System's database.	C	Assistant Administrator for Chemical Safety and Pollution Prevention	5/31/19	

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

Agency Response

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

APR – 9 2019

OFFICE OF CHEMICAL SAFETY
AND POLLUTION PREVENTION

MEMORANDUM

SUBJECT: Response to Draft Report entitled "Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement," Project No. QA-FY17-0091

FROM: Alexandra Dapolito Dunn
Assistant Administrator

TO: Charles J. Sheehan
Acting Inspector General

This memorandum responds to the OIG's Draft Report entitled "Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement," Project No. QA-FY17-0091, dated March 11, 2019.

I. General Comments:

The Office of Chemical Safety and Pollution Prevention (OCSPP), Office of Pesticide Programs (OPP), appreciates the OIG's effort in evaluating the following:

- Determining whether the vulnerability testing of servers that host and manage PRIA and FIFRA applications is complete, and whether the agency is taking actions to correct identified vulnerabilities.

- Determining whether controls exist for the completeness of registrations processed within PRIA and FIFRA systems, and whether fees are recorded in the EPA's Compass Financials.

- Reviewing information technology security of the database containing PRIA and FIFRA information.

OCSPP generally agrees with all the OIG recommendations and plans to implement the following proposed corrective actions. In addition to this response, documentation is being sent to you as evidence of the completion of corrective actions 1, 3, 6 and 7.

II. OCSPP's Response to the Recommendations:

Recommendation 1: Develop and implement internal controls over the manual processes used to post fee payments from Compass Financials to the Pesticide Registration Information System and post fee refunds from the Pesticide Registration Information System to Compass Financials.

> **OCSPP Corrective Action 1:** OPP has developed and implemented internal controls over the manual processes used to post fee payments. This process involves the Team Leader in the Information Services Branch who is responsible for reviewing all posting of fee payments from Compass Financials to PRISM and the Information Services Branch Chief who checks the validity of all fee postings.
>
> - **Completed**: April 2019

Recommendation 2: Identify an automated solution for the manual processes used to post fee payments from Compass Financials to the Pesticide Registration Information System and post fee refunds from the Pesticide Registration Information System to Compass Financials to maintain data integrity. If it is determined to be possible, implement such a solution.

> **OSCPP Proposed Corrective Action 2**: 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.
>
> - **Target Completion Date**: By October 2019, a document of findings will be presented to the OPP senior leadership team for consideration.

Recommendation 3: Implement a formal process for creating plans of action and milestones (POA&Ms) in XACTA and tracking the mitigation of vulnerabilities identified by the Office of Environmental Information.

> **OCSPP Corrective Action 3**: OPP follows the OCSPP's Information Systems Security Officer (ISSO) guidance and formal process for creating Plans of Action and Milestones (POA&Ms) and uploading artifacts into XACTA for PRISM and the OPP LAN. Included in this guidance are key requirements that address mitigation of vulnerabilities

and response timelines as identified by the former Office of Environmental Information (now the Office of Mission Support) and now incorporated into the CIO Policy 2150-P-14.2. The key elements include:

(1) Critical Vulnerabilities—mitigate or remediate within two calendar days. If more than two days are required, create a POA&M.
(2) High Vulnerabilities—mitigate or remediate within 30 calendar days. If more than 30 days are required, create a POA&M.
(3) Moderate Vulnerabilities—mitigate or remediate within 60 calendar days. If more than 60 days are required, create a POA&M.
(4) Low Vulnerabilities—mitigate within 90 calendar days. If more than 90 days are required, create a POA&M.

Tracking POA&Ms: OCSPP's ISSO conducts formal weekly and monthly review meetings for tracking the progress of addressing all unmitigated POA&Ms. Each POA&M and corresponding artifact is tracked, stored, and retrieved using the XACTA repository system which includes pending, new, and past due POA&Ms. Once a POA&M has been fully mitigated and verified by all parties then it can be closed in XACTA by either the OCSPP ISSO or the OPP System Owner.

- **Completed**: October 2018

Recommendation 4: Implement controls to comply with federally required time frames to install patches to correct identified vulnerabilities in the Pesticide Registration Information System.

OCSPP Proposed Corrective Action 4: 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.

- **Target Completion Date**: By October 2019, OPP will update its PRISM and OPP LAN System Security Plan to reflect these procedures.

Recommendation 5: Implement the EPA's patch management process for the Pesticide Registration Information System.

OCSPP Proposed Corrective Action 5: OPP will address this recommendation when the program implements OCSPP's proposed Corrective Action 4.

- **Target Completion Date**: By October 2019, OPP will update its PRISM and OPP LAN System Security Plan(s) to reflect these procedures.

Recommendation 6: Implement periodic review of roles within the Pesticide Registration Information System to determine the appropriateness of privileges assigned to roles and users.

> **OCSPP Corrective Action 6**: OPP's Information Security Officer periodically conducts a review of roles and system privileges in PRISM and the OPP LAN to ensure the appropriate level of access assigned to all users in accordance with EPA's Chief Information Officer Policy CIO 2150-3.
>
> - **Completed**: October 2018

Recommendation 7: Implement procedures for the independent review of administrative access logs for the Pesticide Registration Information System's database.

> **OCSPP Corrective Action 7**: Each year OPP complies with the procedures established by the EPA Chief Information Security Office for the independent review of administrative access logs for all agency IT systems which includes PRISM. This year's independent review of PRISM began on March 18, 2019 and will conclude on or about June 2019.
>
> - **Completed**: March 2019

cc: All OCSPP DAAs
OPP OD, DOD
Kevin Christensen, Assistant Inspector General for Audit and Evaluation
Richard Eyermann, Deputy Assistant Inspector General for Audit and Evaluation
Rudy Brevard, Director, IRMA, OIG
Janet L. Weiner, OCSPP Audit Liaison
Cameo Smoot OPP Audit Liaison
Bobbie Trent, OCFO AFC

Appendix B

Distribution

The Administrator
Associate Deputy Administrator and Chief of Operations
Chief of Staff
Deputy Chief of Staff
Assistant Administrator for Chemical Safety and Pollution Prevention
Principal Deputy Assistant Administrator for Chemical Safety and Pollution Prevention
Deputy Assistant Administrator for Programs, Office of Chemical Safety and Pollution Prevention
Deputy Chief Financial Officer
Associate Chief Financial 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
Director, Office of Continuous Improvement, Office of the Administrator
Director, Office of Pesticide Programs, Office of Chemical Safety and Pollution Prevention
Director, Office of Budget, Office of the Chief Financial Officer
Controller, Office of the Controller, Office of the Chief Financial Officer
Deputy Controller, Office of the Controller, Office of the Chief Financial Officer
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of Chemical Safety and Pollution Prevention
Audit Follow-Up Coordinator, Office of Pesticide Programs, Office of Chemical Safety and Pollution Prevention
Audit Follow-Up Coordinator, Office of the Chief Financial Officer
Audit Follow-Up Coordinator, Office of Budget, Office of the Chief Financial Officer
Audit Follow-Up Coordinator, Office of the Controller, Office of the Chief Financial Officer