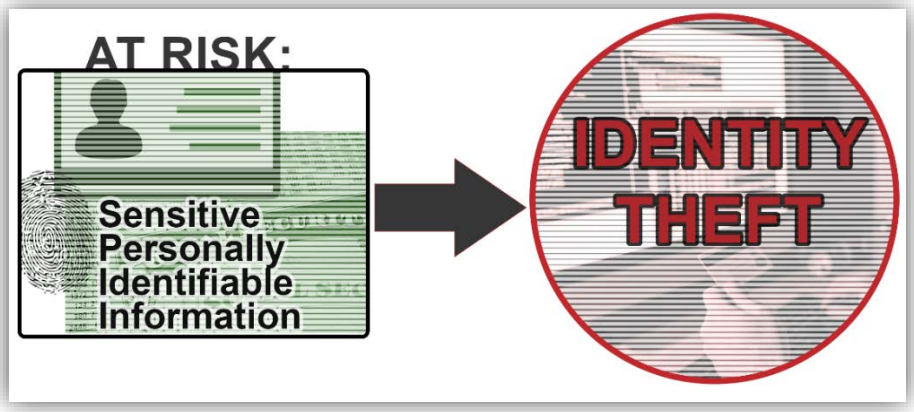
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Hotline Report:
Operating Efficiently and Effectively

Management Alert: EPA's Incident Tracking System Lacks Required Controls to Protect Personal Information

Report No. 18-P-0298 **September 28, 2018**



Report Contributors:

Rudolph M. Brevard
Vincent Campbell
Nancy Dao
Scott Sammons

Abbreviations

CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
OEI	Office of Environmental Information
OIG	Office of Inspector General
PII	Personally Identifiable Information
SORN	System of Records Notice
SPII	Sensitive Personally Identifiable Information
SSN	Social Security Number
TSP	Thrift Savings Plan

Cover Image: The exposure of sensitive personally identifiable information can lead to identify theft. (EPA OIG image)

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

18-P-0298
September 28, 2018

At a Glance

Why We Did This Project

The Office of Inspector General (OIG) for the U.S. Environmental Protection Agency (EPA) conducted this audit in response to an OIG hotline complaint. Our objective was to determine whether the EPA implemented security controls to protect personally identifiable information (PII) processed by the agency's incident tracking system, which is used to troubleshoot information technology issues.

PII is defined as information that can be used to distinguish or trace an individual's identity (such as name, date of birth and address), either alone or when combined with other information that is linked or linkable to a specific individual. Sensitive PII (SPII) is a subset of PII, and includes Social Security numbers or comparable identification numbers, biometric data, and financial or medical information associated with an individual.

This report addresses the following:

- *Operating efficiently and effectively.*

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

Listing of OIG reports.

Management Alert: EPA's Incident Tracking System Lacks Required Controls to Protect Personal Information

What We Found

The EPA's current incident tracking system lacks the required security controls to (1) protect the confidentiality of PII and SPII; and (2) enforce password management requirements, even though the requirements are specified in federal and agency guidance.

The EPA's incident tracking system lacks the required privacy and security controls to protect PII and SPII, which could lead to identity theft.

The EPA was unaware that PII and SPII were included on incident tickets handled by help desk technicians, and retained in the current incident tracking system where it can be viewed by all registered users (EPA employees and contractors). We found that current operating procedures do not instruct help desk technicians to exclude PII and SPII within incident tickets, or to follow the EPA's information security and privacy directives to protect the confidentiality of PII and SPII. As a result, we identified 25 incident tickets within the agency's current incident tracking system. The incident tickets disclosed Social Security numbers, W-2 information, dates of birth, home addresses and Thrift Savings Plan account information.

The EPA began a partial rollout of a replacement incident tracking system in May 2018. The rollout has an anticipated completion date of September 30, 2018. Current standard operating procedures will be used with the replacement incident tracking system as well. Therefore, we are issuing this report to reiterate the need for management to address current weaknesses, so that the weaknesses do not continue to impair the EPA's ability to protect the confidentiality of PII and SPII.

Recommendations and Planned Agency Corrective Actions

We made several recommendations to the Assistant Administrator for Environmental Information. We recommended that the EPA implement a strategy to protect the confidentiality of PII and SPII contained in the EPA's current incident tracking system, and to update standard operating procedures for help desk technicians to follow when handling incident tickets that require collecting PII and SPII.

Throughout the audit process, we worked closely with EPA representatives and kept them informed about any issues identified. On June 5, 2018, we met with agency representatives concerning the OIG's discussion document pertaining to this audit. The agency agreed with Recommendations 1 and 2, and we consider these recommendations resolved with corrective actions pending. Recommendations 3 and 4 are unresolved pending EPA management's response to this report.

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

THE INSPECTOR GENERAL

September 28, 2018

MEMORANDUM

SUBJECT: Management Alert: EPA's Incident Tracking System Lacks Required Controls to Protect Personal Information
Report No. 18-P-0298

FROM: Arthur A. Elkins Jr.

TO: Vaughn Noga, Principal Deputy Assistant Administrator and
Deputy Chief Information Officer
Office of Environmental Information

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). The project number for this audit was OA&E-FY18-0124. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The EPA's Office of Environmental Information, Office of Information Technology Operations, Desktop Support Services Division, is responsible for issues discussed in this report.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report within 60 calendar days. You should include planned corrective actions and completion dates for all recommendations that need additional information for resolution. Your response 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.

The report will be available at www.epa.gov/oig.

Table of Contents

Appendix

Purpose

In response to a hotline complaint, the Office of Inspector General (OIG) for the U.S. Environmental Protection Agency (EPA) conducted this audit to determine whether the EPA implemented security controls to protect personally identifiable information (PII) processed in the agency's incident tracking system.

Background

In December 2017, the OIG received a hotline complaint that alleged the EPA's current incident tracking system "contained PII and Social Security numbers" (SSNs). Allegedly, the PII and SSNs were visible to anyone with access to the system. The complaint further alleged that the system did not comply with the agency's password standards. The OIG researched the merits of the allegations and corroborated the information.

According to the Federal Bureau of Investigation's *2017 Internet Crime Report*, personal data breach (e.g., an individual's sensitive, protected or confidential data that is copied, transmitted, viewed, stolen or used by an unauthorized individual) and identity theft were, respectively, the second- and sixth-highest-ranked internet crimes reported to the Internet Crime Complaint Center by victims in 2017. The report found that victims reported aggregate losses of approximately $77.1 million for personal data breaches and approximately $66.8 million for identity theft.

Office of Management and Budget Circular A-130 (Revised), *Managing Information as a Strategic Resource*, dated July 28, 2016, advises agencies to establish administrative, technical and physical safeguards to protect PII from unauthorized access, use, modification, loss, destruction, dissemination or disclosure. The circular further advises agencies to maintain an inventory of agency information systems that involve PII; regularly review and reduce PII to the minimum necessary; and eliminate the unnecessary collection, maintenance and use of SSNs.

EPA Chief Information Officer (CIO) 2151.1, *Privacy Policy*, provides the following definition of PII:

> [A]ny information about an individual, maintained by an agency, that can be used to distinguish, trace or identify an individual's identity, including personal information which is linked or linkable to an individual (e.g., name, date of birth, address).

The policy defines sensitive PII (SPII) as "a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience or unfairness to an individual." SPII requires additional levels of security controls. The EPA's current incident tracking system is an agencywide tool that manages information system service requests and security incidents. The system tracks and reports these requests and incidents, starting with the reporting of the issue, all the way through the issue's resolution.

EPA definitions for PII and SPII:

PII — Information used to distinguish, trace or identify an individual's identity, such as name, date of birth and home address.

SPII — A subset of PII, this information includes Social Security numbers or comparable identification numbers, and passport, biometric, medical or financial data.

The EPA's incident tracking system contains several modules used to troubleshoot information technology issues. The EPA uses the incident management module within the incident tracking system to document technical issues, such as resetting a user's password, removing a virus from the agency's network or granting user access to an EPA system. Help desk technicians manage incident tickets within the incident management module to document the details of each event and track the resolution. A technician enters as much data as necessary on the incident ticket to help assigned technicians resolve problems. Sometimes the information entered on the incident ticket includes PII or SPII, which can be viewed by all registered users (EPA employees and contractors) of the system.

The EPA is currently implementing a new incident tracking system and plans to retire the current system by September 30, 2018.

Responsible Office

The Office of Environmental Information (OEI) provides enterprise level strategic planning, collaboration, management and accountability for the implementation of the agency's technology. The Office of Information Technology Operations' Desktop Support Services Division, within OEI, manages the current incident tracking system and the replacement system.

Scope and Methodology

We performed our audit from March through September 2018. We conducted this performance audit 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 audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We reviewed federal and EPA policies and procedures on privacy and password management requirements to protect the confidentiality of PII and SPII collected and maintained in the agency information systems. We reviewed these policies and procedures to help determine what constitutes PII and SPII.

We obtained access to the agency's current incident tracking system to conduct queries for incident tickets with PII and SPII. We performed a query on the term "SSN" in the "search" data field. The EPA's incident tracking system identified a total of 2,060 tickets that matched the term "SSN." We judgmentally selected a sample of 264 tickets to determine whether PII and SPII appeared within each ticket. The incident tickets were dated from fiscal years 2009 to 2015.

We reviewed recent security assessment reports, privacy impact assessments, and system security plans for the current and replacement incident tracking systems to determine whether (1) the systems' security documentation indicated PII would be collected, and (2) password management controls complied with EPA requirements. We interviewed agency personnel responsible for the oversight, management and implementation of the current and replacement incident tracking systems. We also interviewed contract personnel who manage the current and replacement incident tracking systems on behalf of the EPA to determine what security controls are currently in place to protect the confidentiality of PII and SPII.

Results

We found that the current incident tracking system lacked required controls to protect sensitive data and manage passwords used to access the system. We identified 25 incident tickets that contained PII and SPII (e.g., SSNs, date of birth and W-2 information) for 73 individuals within the agency's current incident tracking system. Federal and EPA guidance require system owners to take steps to prevent the unauthorized access, use, modification, loss, destruction, dissemination or disclosure of PII and SPII. The incidents occurred because the EPA did not include guidance within its current operating procedures to instruct help desk technicians to not include PII and SPII within incident tickets. Further, as of September 2018, the EPA has not yet identified a solution to enforce the agency's password requirements for the current incident tracking system, even though the system's password module has been inoperable since a software upgrade in 2016.

The EPA began a partial rollout of a replacement incident tracking system in May 2018. The rollout has an anticipated completion date of September 30, 2018. Current standard operating procedures also will be used with the replacement incident tracking system. Therefore, we are issuing this report to reiterate the need for management to address current weaknesses, so that the weaknesses do not continue to impair the EPA's ability to protect the confidentiality of PII and SPII.

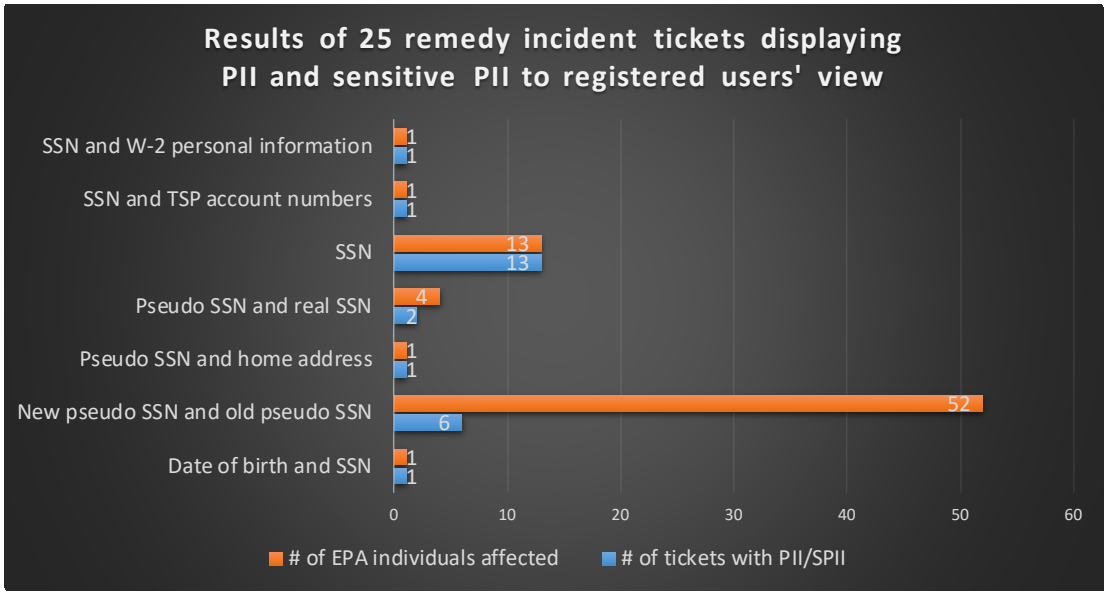
Confidentiality of Personal Information Is Not Protected in EPA's Incident Tickets

The EPA's incident tickets contain personal information that is visible to all registered users of the current incident tracking system. Based on our review of 264 tickets that contained the term "SSN," we found that 25 incident tickets (9 percent) contained PII and SPII. Some incident tickets included multiple individuals' PII or SPII. The 25 incident tickets contained PII and SPII on 73 individuals, and included the following information:

- Social Security numbers.
- W-2 personal information.
- Pseudo SSNs (issued by the Office of Personnel Management to non-United States citizens for background investigation purposes).
- Dates of birth.
- Home addresses.
- Thrift Savings Plan (TSP) account numbers. (The TSP is a retirement savings and investment plan for federal employees.)

Figure 1 shows the breakdown of PII and SPII found in the 25 incident tickets.

Figure 1: Examples of PII and SPII found in incident tickets



Source: OIG compiled using EPA incident tracking system data.

EPA CIO 2151.1, *Privacy Policy*, dated September 14, 2015, states that EPA employees, managers, contractors and grantees working on behalf of EPA will:

- Ensure that PII contained in a system of records, to which they have access in the performance of their duties, is protected so that the security and confidentiality of the information are preserved.
- Access and use only information for which they have official authorization.

We met with OEI personnel to discuss and present the contents of the incident tickets we selected for our sample. OEI personnel were unaware of PII and SPII documented within the incident tickets and were unsure why help desk technicians were entering this information. After further examining ticket content, OEI personnel concluded that the nature of documenting PII and SPII appeared to be associated with personnel providing the information to technicians to correct payroll and human resource records.

After additional correspondence with OEI personnel, we learned that the office did not include guidance within its current operating procedures to instruct help desk technicians to not include or maintain PII and SPII within incident tickets. We also learned that the OEI did not follow EPA information security and privacy directives to protect the confidentiality of PII and SPII if there is a need to collect or maintain this information. OEI personnel stated that operating procedures need to be updated to provide clear instructions to help desk technicians and how they are to handle incident tickets that involve PII and SPII.

Under the OEI's current incident tracking system, the security assessment report (dated August 2017) and the privacy impact assessment (dated January 2016) documented the system would not collect PII. As a result, the OEI did not conduct periodic reviews of incident tickets to verify whether PII and SPII were collected or stored within its current incident tracking system. If periodic reviews had been performed, the EPA could have determined whether a System of Records Notice (SORN) was needed.

A SORN informs management that a system containing privacy information may require additional security controls as required by National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013; and EPA CIO 2151-P-03.1, *Procedures for Preparing and Publishing Privacy Act Systems of Records Notices*, dated January 5, 2010.

The OEI has started a transition to a new system to replace the current incident tracking system. The replacement system became operational in May 2018 for select agency locations. The security assessment report for the replacement system (dated January 2018) indicated that the replacement system would not

collect PII. However, the privacy impact assessment and the draft system security plan state that the new system does collect PII. We are uncertain about the accuracy of any of this documentation, since management was not aware that PII and SPII were included in the current tracking system until we brought this issue to their attention. EPA personnel stated that the replacement and current incident tracking systems will both be in operation until September 30, 2018.

The EPA could incur additional costs putting security controls in place to protect individuals' identities within the current incident tracking system until it is decommissioned. The EPA also could be subject to lawsuits because the agency did not perform due diligence to protect the confidentiality of the 73 individuals' PII and SPII from unauthorized use and theft. Since incident tickets associated with those individuals were annotated as resolved and closed between fiscal years 2009 and 2015, those individuals' personal information was exposed for at least 3 years, as of September 2018. Exposure of the individuals' PII and SPII could lead to identity theft and result in financial harm, embarrassment or inconvenience.

EPA's Incident Tracking Systems Do Not Comply with Internal Password Management Controls

The current incident tracking system is not configured to meet the agency's password management length, character and life span requirements. In January 2018, we requested access to the system and were provided a simple six-character password. Upon initially logging into the system, we were not prompted to change the initial temporary password. We maintained the simple six-character password for more than 60 days without the system requiring us to change our password. Even though the system did not meet password requirements, the agency also did not request a password requirement waiver as required by the agency's information security directive. Furthermore, the incident tracking system's security plan, dated January 2016, indicates that password management controls have been implemented; however, the plan has not been updated to reflect the current weakness in password controls.

EPA CIO 2120-P-07.2, *Information Security - Identification and Authentication Procedure,* dated November 30, 2015, requires specific password characteristics: be comprised of 12 characters; include upper- and lower-case letters, as well as numbers and special characters; and have a maximum password life span of 60 days. Temporary passwords can be used to facilitate password changes or initial account establishment if the system forces an immediate change.

If password guidelines cannot be met, a request can be made for a waiver of the password requirements and standards, and the request must include, at a minimum, specific designation of which requirement(s) the waiver request is addressing. EPA CIO 2150.3-P-12.1, *Information Security - Interim Planning Procedures, V3.6,* dated August 6, 2012, holds the system owner responsible for

reviewing and updating the system security plan when significant changes occur to the system's operating environment or security requirements.

OEI personnel indicated that a waiver outlining the system's noncompliance with agency password requirements was not initiated when the password module failed during the 2016 software upgrade because the software vendor provided a patch to fix the issue. However, OEI personnel stated that the patch did not correct the issue. An EPA contract representative stated that, as of April 2018, the development and testing of a remediation for the password configuration problem is in progress with a target deployment to the production environment as soon as possible.

We also discovered that password management controls documented in the replacement system's draft security plan (dated March 2018) did not meet EPA requirements. We found the following issues with the replacement system's password management controls:

- Password expiration requirements were stated as every 90 days instead of the policy requirement of every 60 days.
- Minimum password length requirements were eight characters instead of the required 12 characters.

OEI personnel stated that they were aware of the inconsistency and that the system's draft security plan had been updated. OEI personnel provided us with a copy of the updated draft security plan dated April 11, 2018, which included language consistent with the EPA's password management requirements, but personnel stated that the replacement system's security plan was a work-in-progress.

Password management is an additional cybersecurity control that can protect data from unauthorized access, use and destruction. Since the current incident tracking system contains SPII, it is essential that required password controls are implemented to impede internal and external threats from compromising the system and obtaining access to personal information.

Agency Actions

After our June 5, 2018, meeting with EPA representatives, the agency stated that it had resolved the password management issue with the current incident tracking system. EPA representatives provided information that indicated the current system will require a password of at least 12 characters and a new password will expire in 60 days. We concluded that the updated password length requirement is being enforced.

Conclusion

Without proper privacy and security controls in place to make sensitive information unusable, PII and SPII are vulnerable to unauthorized access. The lack of these controls can provide cyber thieves an opportunity to exploit the integrity of the EPA's information security posture and compromise the confidentiality of personal data maintained in the agency's systems.

Recommendations

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.

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.

3. Complete a System of Records Notice for the replacement incident tracking system.

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.

Agency Response and OIG Evaluation

On May 23, 2018, we issued a discussion document outlining our findings and recommendations to the EPA. We met with agency representatives to discuss our findings and recommendations on June 5, 2018. Agency representatives stated that the OEI would not provide written responses to the discussion document. Agency representatives further stated that their verbal responses would serve as their official responses to the discussion document.

The agency agreed with our recommendations. EPA representatives stated that mitigation activities are underway to address the report's findings, such as:

- Retraining help desk technicians on the correct procedures for handling PII and SPII when this information is submitted to the EPA's help desk.

- Updating standard operating procedures for handling PII and SPII to comply with EPA privacy policies and procedures.
- Redacting PII and SPII in incident tickets retained in the EPA's current incident tracking system.
- Formulating a plan to mitigate the password deficiencies in the current incident tracking system.

A target date of September 30, 2018, has been established to redact all PII and SPII from incident tickets, disconnect the current incident tracking system from the agency's network, and archive that system's database. EPA representatives said that there is a possibility the September 30, 2018, target date to implement the strategy may not be met if there are issues with the ongoing rollout of the replacement system. However, the EPA's goal is not to exceed the target date since keeping the current tracking system online would present an additional risk and cost to the agency. EPA representatives further stated that help desk technicians will use the updated standard operating procedures for handling PII and SPII in the replacement incident tracking system.

Recommendation 1 is resolved since the EPA plans to implement a strategy to redact PII and SPII in incident tickets, and disconnect the current incident ticketing system from the network by September 30, 2018. Recommendation 2 is resolved since EPA management indicated that standard operating procedures were updated on July 31, 2018, and they provided a copy of the updated procedures. Planned corrective actions are pending in relation to the EPA establishing controls to verify PII and SPII are not documented in incident tickets.

In response to the OIG's original recommendation for the agency to complete a SORN for both the current and replacement systems, an EPA representative stated that conducting a SORN is a lengthy process, and considering the current system is being decommissioned in September 2018, it would not be feasible to complete a SORN for the current system. However, the representative also said that the agency is in the process of completing a SORN for the replacement system. The OIG then revised Recommendation 3 to require the EPA to complete a SORN for the replacement incident tracking system. The recommendation was modified to emphasize the work that needs to be completed on the new system. The EPA has yet to provide a date for when it will complete this corrective action. Recommendation 3 is unresolved since the EPA did not provide any planned corrective actions with milestone dates.

EPA representatives did not have any comments regarding Recommendation 4. This recommendation is unresolved since the EPA did not provide any planned corrective actions with milestone dates.

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	8	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.	R	Assistant Administrator for Environmental Information	9/30/18	
2	8	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.	R	Assistant Administrator for Environmental Information	7/31/18	
3	8	Complete a System of Records Notice for the replacement incident tracking system.	U	Assistant Administrator for Environmental Information		
4	8	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.	U	Assistant Administrator for Environmental Information		

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

Appendix A

Distribution

The Administrator
Deputy Administrator
Special Advisor, Office of the Administrator
Chief of Staff
Chief of Operations
Assistant Administrator for Environmental Information
Principal Deputy Assistant Administrator for Environmental Information
Deputy Assistant Administrator for Environmental Information
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 Information Technology Operations, Office of Environmental Information
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of Environmental Information