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.