



At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency (EPA) must safeguard individuals' Personally Identifiable Information (PII) consistent with the Privacy Act, the E-Government Act of 2002, Office of Management and Budget (OMB) directives, and other federal requirements. Without the proper security controls, the PII is vulnerable to unauthorized access and use.

We sought to determine whether the EPA has developed and implemented policies, procedures and processes for protecting sensitive PII in accordance with federal and agency criteria.

This report addresses the following EPA theme:

- *Embracing EPA as a high performing organization.*

For further information, contact our public affairs office at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2014/20140224-14-P-0122.pdf

EPA Needs to Improve Safeguards for Personally Identifiable Information

What We Found

The EPA has not created formal policies and procedures for several processes that contribute to the safeguarding of PII and that ensure compliance with federal requirements. The EPA is using an inaccurate list of systems that contain sensitive PII to report to OMB and the Chief Information Officer. This listing was not up-to-date and it contained incorrect data about systems. Having outdated information may lead OMB and agency management to make decisions that may not be applicable to the agency's needs. The lack of formal policies and procedures and management oversight over agency processes for safeguarding of PII does not ensure employees are aware of their responsibilities for protecting PII.

The lack of stronger privacy program processes and procedures places the EPA's sensitive PII at a greater risk of compromise and misuse.

The PII training process covered 50 percent of the prescribed topics and did not track training of agency personnel. Federal guidance provides specific training topics and directs agencies to train employees on their privacy responsibilities. The agency had not set up a process to track training completion and had not evaluated available privacy training before contracting to develop a new privacy training program. As a result, EPA employees are only trained on a portion of the requirements and management is unable to assess whether all employees have been trained.

Recommendations and Planned Corrective Actions

We recommend that the EPA implement a "rules and consequences" procedure for safeguarding PII; develop policies and procedures for matching programs; develop and implement a process for maintaining an accurate, current listing of systems that contain sensitive PII; implement a process to train individuals who access PII; and conduct reviews of available training before the agency enters into contracts.

The agency concurred with the report's recommendations and provided corrective action plans, which we found acceptable. The agency initially did not agree with recommendation 6 of the draft report and proposed an alternative corrective action. We met with agency officials and revised recommendation 6, and the agency concurred with the revised recommendation.

Noteworthy Achievements

The EPA had created a privacy program as we recommended in a prior Office of Inspector General audit and provided a memorandum to us certifying completion of report recommendations.