Office of Inspector General
U.S. Environmental Protection Agency
At a Glance

21-E-0226
September 13, 2021

Why We Did This Evaluation

We performed this evaluation to determine whether the system security plans in the Office of the Chief Financial Officer, the Office of Land and Emergency Management, and the Office of Research and Development are developed and updated in accordance with National Institute of Standards and Technology guidance.

System security plans are required for all information systems. The National Institute of Standards and Technology states that major applications require "special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application." The plans should document an information system's security categorization and include an inventory of the system's minor applications, which are similar to major applications but do not require "special attention."

This evaluation supports an U.S. Environmental Protection Agency mission-related effort:

- *Operating efficiently and effectively.*

This evaluation addresses top EPA management challenges:

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

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

List of OIG reports.

EPA's Emergency Response Systems at Risk of Having Inadequate Security Controls

What We Found

If the availability and integrity of emergency response system data are jeopardized, it could harm the EPA's ability to coordinate response efforts to protect the public from environmental disasters.

The EPA did not follow the National Institute of Standards and Technology guidance in determining and documenting the justification for the security categorizations of five emergency response systems. Further, the EPA's security categorization process did not include key participants, as recommended by NIST. In addition, security documentation for some of the EPA's minor applications did not exist.

NIST requires that agencies develop system security plans for all information systems, including major applications and general support systems, and tailor the systems' security controls based on the systems' security categorization. A system with a high-security categorization would require greater security controls than a system with a moderate- or low-security categorization. NIST guidance provides that security controls specific to minor applications should be documented in a system security plan as an appendix or in a paragraph. NIST also provides that all applications be secure and free of vulnerabilities.

The EPA's staff and managers may not fully understand NIST requirements because the Agency's security training does not cover the NIST security categorization process. The EPA's security categorization guidance referenced NIST but did not describe the steps EPA personnel should take to implement NIST guidance. Additionally, the EPA has not implemented controls or oversight to assure that NIST guidance was followed. EPA systems are more vulnerable to security threats if the Agency does not follow NIST guidance when categorizing security levels for systems or documenting system security. Such threats could compromise a system's data and negatively impact the EPA's ability to respond to emergencies.

Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Land and Emergency Management implement controls to follow NIST guidance when conducting system categorizations. We recommend that the assistant administrator for Research and Development implement a process to list and describe all minor applications in the appropriate system security plan. We also recommend that the assistant administrator for Mission Support provide role-based training that covers system security categorizations and implement a process to document that tools and models are secure. The Agency concurred with five of the seven recommendations and provided acceptable corrective actions and estimated milestone dates. Two recommendations remain unresolved with resolution efforts in progress.