U.S. Environmental Protection Agency
Office of Inspector General

21-E-0124
April 16, 2021

At a Glance

Why We Did This Evaluation

We performed this evaluation to assess the U.S. Environmental Protection Agency's compliance with the *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

The fiscal year 2020 *IG FISMA Reporting Metrics* outlines five security function areas and eight corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which IGs should rate agency information security programs:

- Level 1, Ad Hoc.
- Level 2, Defined.
- Level 3, Consistently Implemented.
- Level 4, Managed and Measurable.
- Level 5, Optimized.

This evaluation addresses the following:

- *Compliance with the law.*
- *Operating efficiently and effectively.*

This evaluation addresses top EPA management challenges:

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

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

List of OIG reports.

EPA Needs to Improve Processes for Updating Guidance, Monitoring Corrective Actions, and Managing Remote Access for External Users

What We Found

We concluded that the EPA achieved an overall maturity level of Level 3 (Consistently Implemented) for the five security functions and eight domains outlined in the *FY 2020 IG FISMA Reporting Metrics*. This means that the EPA consistently implemented its information security policies and procedures, but quantitative and qualitative effectiveness measures are lacking. We found that the EPA has deficiencies in the following areas:

Deficiencies in the EPA's information technology internal controls could be used to exploit weaknesses in Agency applications and hinder the EPA's ability to prevent, detect, and respond to emerging cyberthreats.

- Completing reviews of its outdated information security procedures by the established deadlines or making plans to complete a review at a later date.
- Verifying corrective actions are completed as represented by the Agency and not falsely reporting related resolutions.
- Enforcing established information system control requirements for the Agency's web application directory system that allows external users access to EPA applications, including the grants and Superfund management systems.

Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Mission Support (1) establish a control to update information technology procedures to make them consistent with current federal directives, (2) take steps to require that the audit follow-up coordinator has the capability to verify when corrective actions are completed before the action official closes audit reports in the Agency's audit tracking system, (3) implement a control for authorization and recertifying users' access for the web application directory system, (4) implement procedures to monitor privileged users' activities for unusual or suspicious activity, and (5) establish a governance structure to support the Agency's identity, credential, and access management program efforts as required by the Office of Management and Budget.

The EPA agreed with our five recommendations; completed corrective actions for two of them; and provided acceptable planned corrective actions and estimated milestone dates for the remaining three, which we consider resolved with corrective actions pending.