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

22-P-0010
December 8, 2021

Why We Did This Audit

The Office of Inspector General conducted this audit to determine whether the (1) U.S. Environmental Protection Agency completed corrective actions for agreed-to cybersecurity audit recommendations in OIG reports issued from fiscal year 2017 through fiscal year 2020 and (2) corrective actions effectively resolved the weaknesses identified.

The OIG has identified *Enhancing Information Technology Security to Combat Cyberthreats* as a key management challenge confronting the EPA. The OIG has a responsibility to detect and prevent mismanagement and misconduct in the EPA's programs and operations. The OIG achieves this, in part, by confirming that agreed-to corrective actions to address OIG report recommendations and findings were completed by the Agency.

This audit supports an EPA mission-related effort:

- *Operating efficiently and effectively.*

This audit addresses top EPA management challenges:

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

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

List of OIG reports.

EPA Generally Adheres to Information Technology Audit Follow-Up Processes, but Management Oversight Should Be Improved

What We Found

The EPA's goal to provide its workforce and the public with accurate information is undermined when the Agency does not correct deficiencies in a timely manner, which weakens the integrity of its systems and data.

The EPA completed the 13 corrective actions for cybersecurity audit recommendations in the OIG reports that we reviewed as part of this audit. However, for one of the 13 corrective actions, the EPA inaccurately reported its timely completion. For two of the 13 corrective actions, the EPA lacked management oversight to effectively resolve identified weaknesses. We found that the EPA has deficiencies in the following areas:

- Verifying compliance with annual training requirements for information technology contractors with significant information security responsibilities.
- Verifying corrective actions were completed as represented by the Agency.
- Deploying patches to mitigate identified vulnerabilities in the Agency's Pesticide Registration Information System database in a timely manner.

Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Chemical Safety and Pollution Prevention develop a strategy to validate that corrective actions are completed before closing them in the Agency's audit tracking system and implement controls to comply with federal and Agency required time frames to install patches. In addition, we recommend that the assistant administrator for Mission Support develop and implement processes for storing certifications collected for annual role-based training requirements in a centralized restricted location.

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

—National Institute of Standards and Technology's *Glossary*

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