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

22-E-0028
March 30, 2022

The EPA Lacks Documented Procedures for Detecting and Removing Unapproved Software on the Agency's Network

Why We Did This Evaluation

We performed this evaluation to assess the U.S. Environmental Protection Agency's compliance with the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* and determine whether the EPA followed its processes to investigate and remove unapproved software from the network.

The reporting metrics outline five security function areas and nine corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which inspectors general should rate their agencies' information security programs:

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

This evaluation supports EPA mission-related efforts:

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

This evaluation addresses a top EPA management challenge:

- *Protecting information technology and systems against cyberthreats.*

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

List of OIG reports.

What We Found

We concluded that the EPA achieved an overall maturity level of Level 3 (Consistently Implemented) for the five security functions and nine domains outlined in the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (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 identified that the EPA has deficiencies in documenting software management procedures on the detection and removal of nonbase software, which is software that is not part of the standard Agency package.

Without documented procedures governing software management and vulnerability remediation processes, the EPA continues to be at risk of outsiders gaining access to compromise and exploit Agency systems and data.

Recommendations and Planned Agency Corrective Actions

We recommend that the Office of Mission Support document procedures to detect and remove unapproved software on the Agency's network and provide targeted training on those procedures. The Agency agreed and provided acceptable planned corrective actions with estimated completion dates to address the recommendations.

Noteworthy Achievement

The Agency developed a software triage team in response to an August 2019 chief information officer memorandum to senior information officers asking them to certify software on the EPA network. The software triage team maintains an agencywide dashboard available to all information management officers that shows all software loaded on program office and regional computers. The team meets regularly to discuss the justification for unapproved software discovered on the network or the information management officers' plans for software removal and updates the dashboard accordingly.