U.S. Environmental Protection Agency
Office of Inspector General

20-E-0309
September 10, 2020

At a Glance

Why We Did This Project

The U.S. Environmental Protection Agency's Office of Inspector General performed this evaluation to (1) assess the completeness of the EPA's processes for testing its network to identify potential vulnerabilities that could compromise the Agency's systems and data, and (2) conduct an independent automated vulnerability testing of information technology resources connected to the EPA's network to identify vulnerabilities that could compromise the confidentiality, integrity, and availability of Agency information systems and data.

We performed our evaluation at EPA headquarters, Region 8, and the National Computer Center. Due to travel restrictions, we only performed OIG vulnerability testing at the Region 8 headquarters and laboratory and on the Region 8 Superfund Cost Recovery Package Imaging and Online System, known as SCORPIOS, server.

This report addresses the following:

- *Operating efficiently and effectively.*

This report addresses a top EPA management challenge:

- *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 Needs to Improve Processes for Securing Region 8's Local Area Network

What We Found

Exploitation of vulnerabilities may result in the loss of confidentiality, integrity, and availability of personally identifiable information and scientific data.

The vulnerability tests of Region 8's local area network, conducted by the EPA's Office of Mission Support, were not comprehensive. Additionally, wireless networks operating within the Region 8 laboratory could jeopardize controls protecting vulnerable laboratory equipment. If vulnerabilities at Region 8 are exploited, there could be denial-of-service attacks, unauthorized disclosure of personally identifiable information, and corruption of scientific data that are used to make program decisions.

The lack of updated SCORPIOS technical documentation, the Office of the Chief Financial Officer's inability to identify whether personally identifiable information is secured on regional SCORPIOS servers, and the security concerns raised in two 2019 hotline complaints regarding SCORPIOS warrant an OCFO investigation of whether SCORPIOS needs additional controls to protect the confidentiality, integrity, and availability of the system. A future breach to the SCORPIOS application could cost the EPA $11,477,250.

Recommendations and Planned Agency Corrective Actions

We recommend that Region 8 update its local area network system security plan and review wireless access points within the Region 8 laboratory. We further recommend that the Office of Mission Support review and implement procedures to verify that vulnerability tests and their results are comprehensive. We also recommend that the OCFO implement internal controls to protect personally identifiable information and manage system development for the SCORPIOS application.

The Agency concurred with our recommendations and provided acceptable corrective actions. The Agency has completed corrective actions for four of our seven recommendations. We consider the remaining three recommendations resolved with corrective actions pending.