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

23-P-0003
November 21, 2022

The EPA Met 2018 Water Security Requirements but Needs to Improve Oversight to Support Water System Compliance

Agency Office of Inspector General conducted this audit to assess the adequacy of the cybersecurity baseline information that the EPA developed to meet the requirements of section 2013 of the America's Water Infrastructure Act of 2018, as well as to determine how community water systems used this information. We also sought to assess the adequacy of EPA oversight to ensure that the water systems are complying with the Act.

Section 2013 requires that the EPA provide baseline information on malevolent acts of relevance to water systems and collect certifications of compliance with the Act. Water systems are to assess their risk and resilience; prepare emergency response plans; certify to the EPA that they completed the initial assessment and plan; and certify to the EPA every five years thereafter that they reviewed, and updated as necessary, their assessments and plans.

This audit supports the following EPA mission-related efforts:

- *Ensuring clean and safe water.*
- *Compliance with the law.*

This audit addresses these top EPA management challenges:

- *Protecting information technology and systems against cyberthreats.*
- *Managing infrastructure funding and business operations.*

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

List of OIG reports.

What We Found

If water systems do not complete risk and resilience assessments or emergency response plans, they are more vulnerable to cyberattacks and other malevolent acts. The 19 percent of water systems that did not certify completion of these assessments and plans serve 40 million people.

The EPA met the requirements of section 2013 of the America's Water Infrastructure Act of 2018, or AWIA, to consult with stakeholders and develop malevolent acts baseline information by August 2019. The EPA updated its baseline information 18 months later in response to an increase in the frequency of cyberattacks. However, the AWIA-imposed deadlines for medium and large water systems to complete their risk and resilience assessments had passed and the systems were not required to update their assessments.

Approximately 19 percent of water systems did not certify that they had completed their risk and resilience assessments by the statutory deadlines. These noncompliant water systems may not be aware of their vulnerability to malevolent acts that could result in loss of service or unsafe drinking water. Furthermore, 95 percent of the noncompliant water systems were small water systems and noncompliant small water systems more likely served disadvantaged communities than compliant systems.

The EPA did not provide adequate oversight to ensure the compliance of water systems—particularly small water systems—with AWIA requirements. Specifically, the EPA did not maintain accurate contact information for water systems, publish guidance regarding enforcement actions against noncompliant water systems, provide sufficient assistance to support small water system compliance, or review the quality of the risk and resilience assessments and emergency response plans. Water systems may therefore fail to meet AWIA requirements and may not understand their vulnerability to malevolent acts.

Recommendations and Planned Agency Corrective Actions

We recommend that the EPA (1) update and implement a plan to support AWIA compliance, (2) update processes to maintain accurate contact information for water systems and to record noncompliance with AWIA, (3) review risk and resilience assessments and emergency response plans to identify improvements, and (4) develop guidance that describes AWIA requirements. The EPA disagreed with our recommendations. The recommendations remain unresolved with resolution efforts in progress. The EPA also provided technical comments. We revised our report as appropriate.