Evaluation of the Use of Infrastructure Investment and Jobs Act Funds for Drinking Water Security Projects

May 5, 2026 | Report No. 26-E-0029

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

Abbreviations

C.F.R.	Code of Federal Regulations
DWSRF	Drinking Water State Revolving Fund
EPA	U.S. Environmental Protection Agency
FY	Fiscal Year
GAO	U.S. Government Accountability Office
IIJA	Infrastructure Investment and Jobs Act
IUP	Intended Use Plan
NSM	National Security Memorandum
OIG	Office of Inspector General
OWSRF	Office of Water State Revolving Fund
PPD	Presidential Policy Directive
SCADA	Supervisory Control and Data Acquisition
SRF	State Revolving Fund
U.S.C.	United States Code

Cover Image

A network being hacked with ransomware. (iStock.com/solarseven)

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, D.C. 20460
(202) 566-2391
www.epa.gov/oig

26-E-0029
May 5, 2026

At a Glance

Evaluation of the Use of Infrastructure Investment and Jobs Act Funds for Drinking Water Security Projects

Why We Did This Evaluation

To accomplish this objective:

The U.S. Environmental Protection Agency Office of Inspector General conducted this evaluation to determine the extent to which Drinking Water State Revolving Fund Infrastructure Investment and Jobs Act supplemental funds are used for projects that improve resilience to physical and cyber threats and hazards.

Water and wastewater systems are critical infrastructure in the United States. However, these water and wastewater systems face risks from malevolent acts and natural hazards, and disruption in system service or destruction of these systems would negatively affect national security, economic stability, and public health and safety. The Infrastructure Investment and Jobs Act included $50 billion to strengthen water infrastructure. This investment included $11.71 billion for the Drinking Water State Revolving Fund Program, $3.8 billion of which was allocated in fiscal years 2022 and 2023. The EPA urged states to use the significant increase in funds to foster water system resilience to all threats and hazards.

To support this EPA mission-related effort:

- *Ensuring clean and safe water.*

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

List of OIG reports.

What We Found

The EPA has opportunities to improve its oversight of physical or cyber resilience projects. Such oversight would help the Agency meet and track strategic goals and requirements to safeguard water and wastewater critical infrastructure. Projects that intend to improve physical security or cybersecurity cannot be identified unless a state includes relevant information about the project in its intended use plan, or IUP, or in Office of Water State Revolving Fund, or OWSRF, database reporting. We analyzed the IUPs that states used to apply for Drinking Water State Revolving Fund Infrastructure Investment and Jobs Act, or IIJA, general supplemental capitalization grants in fiscal years 2022 and 2023 for descriptions of efforts to foster water system resilience to physical and cyber threats. Specifically, we searched for keywords that we expected to see in such descriptions. While the Agency did not require states to include these keywords in their IUPs, if a state described efforts to foster water system resilience in an IUP using expected keywords, then that could indicate the state's intention to use the IIJA funds for projects that improve physical and cyber safeguards.

In the analyzed IUPs, we identified projects and efforts to improve resilience to physical and cyber threats and hazards. While we found descriptions of such projects and efforts, we could not identify the total amount of IIJA funds intended for these purposes because the EPA does not require states to include this information in their IUPs. Moreover, states generally did not describe resiliency efforts in the OWSRF database project descriptions. From our review of the IUPs and OWSRF database project descriptions, we could not determine whether resilience efforts are occurring but are not being described using the expected keywords or whether they are not occurring and thus not described at all. Ultimately, the IUPs and OWSRF database project descriptions that do not describe, using expected keywords, states' efforts to foster water system resilience to physical and cyber threats indicate that the $3.8 billion in IIJA funds allocated in fiscal years 2022 and 2023 may not be prioritized for resilience improvements.

> **Without investments in resilience-related projects, U.S. water systems remain at risk from physical and cyber threats and hazards.**

Recommendations and Planned Agency Corrective Actions

We make two recommendations to the assistant administrator for Water: (1) adopt a method for tracking projects that aim to improve resilience to physical and cyber threats and (2) collaborate with state stakeholders to develop guidance for IUPs. The Agency agreed with our recommendations. We found that the Agency's corrective action partially met the intent of Recommendation 1, which we consider unresolved. We consider Recommendation 2 resolved pending implementation of the agreed-to corrective actions.

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

May 5, 2026

MEMORANDUM

SUBJECT: Evaluation of the Use of Infrastructure Investment and Jobs Act Funds for Drinking Water Security Projects
Report No. 26-E-0029

FROM: Nicole N. Murley, Deputy Inspector General performing the duties of the Inspector General

TO: Jessica L. Kramer, Assistant Administrator
Office of Water

This is our report on the subject evaluation conducted by the U.S. Environmental Protection Agency Office of Inspector General. The project number for this evaluation was OSRE-FY24-0105. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

In accordance with EPA Manual 2750, your office provided acceptable planned corrective actions and estimated milestone dates for Recommendation 2. This recommendation is resolved. A final response pertaining to this recommendation is not required; however, if your office submits a response, it will be posted on the OIG's website, along with our memorandum commenting on the response.

Action Required

Recommendation 1 is unresolved. EPA Manual 2750 requires that recommendations be resolved promptly. Therefore, we request that the EPA provide us within 60 days its response concerning specific actions in process or alternative corrective actions proposed for the recommendation. This response will be posted on the OIG's website, along with our memorandum commenting on the response. The response should be provided as an Adobe PDF file that complies with the requirements of section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that your office does not want released to the public; if the response contains such data, your office should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epa.gov/oig.

Table of Contents

Chapters

Appendixes

Chapter 1
Introduction

Purpose

The U.S. Environmental Protection Agency Office of Inspector General initiated this evaluation to determine the extent to which Drinking Water State Revolving Fund, or DWSRF, Infrastructure Investment and Jobs Act, or IIJA, supplemental funds are used for projects that improve resilience to physical and cyber threats and hazards.

Background

Water and Wastewater Critical Infrastructure Face Risks

The supply of water and the management of wastewater are vital to the United States, and disruption, corruption, or dysfunction related to these activities would have a debilitating effect on national security, economic stability, and public health and safety. Therefore, water and wastewater systems are considered critical infrastructure. In 2024, multiple media accounts highlighted the ongoing and emerging risks of physical or cyber intrusions affecting critical infrastructure. For example, a July 2024 break-in at a water treatment facility in Michigan resulted in so much vandalism that the county had to issue a "Do Not Drink" advisory for residents. As another example from that same time frame, flights by unmanned aerial systems, commonly referred to as drones, over sensitive civilian and military sites in the United States resulted in several airspace restrictions over and around critical infrastructure, including water infrastructure.

Further, the U.S. Government Accountability Office, or GAO, has identified increasing vulnerability to cybersecurity-related risks in the 170,000 water systems across the United States from both cybercriminals and other nations. Such threats to critical infrastructure were the subject of a letter dated March 18, 2024, from the EPA and the National Security Council to state governors. To illustrate the importance of reducing cybersecurity risks, the letter referenced two malicious cyberattacks against drinking water systems in the United States. In 2022, the then-assistant administrator for Water issued a memorandum that urged states to fund projects that foster resilience to all threats and hazards.[1] This call was consistent with objective 5.1 in the *FY 2022-2026 EPA Strategic Plan* to ensure safe drinking water and reliable water infrastructure and to protect public health from the risks of cyber threats to drinking water.

The definition of critical infrastructure in the United States has changed over time, but the first formal federal definition of the term was issued in 1996 in Executive Order 13010, *Critical Infrastructure Protection*.[2] Five years later, the Uniting and Strengthening America by Providing Appropriate Tools

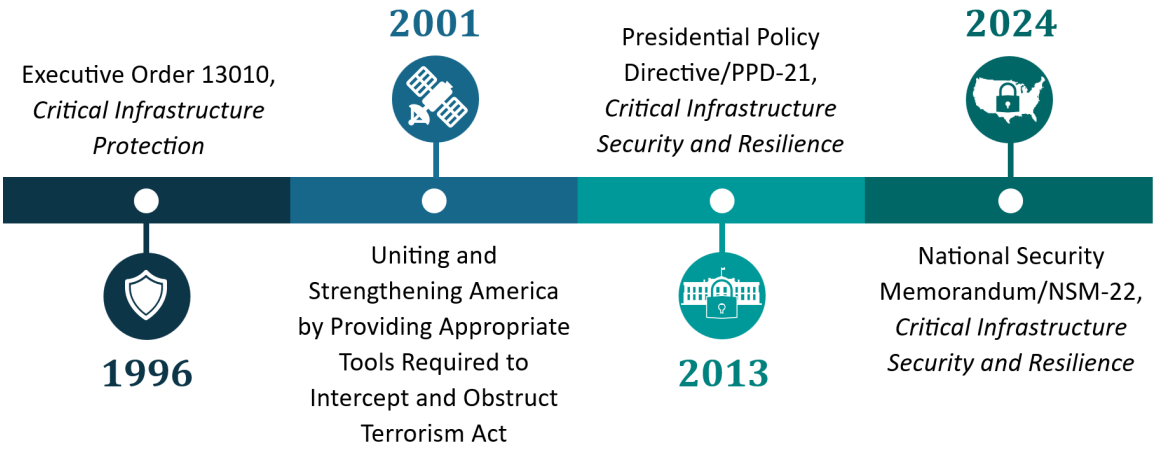
[1] In this report, we refer to these threats and hazards as physical and cyber threats.
[2] Exec. Order No. 13010, 61 Fed. Reg. 37347 (Jul. 15, 1996).

Required to Intercept and Obstruct Terrorism Act of 2001 provided a definition for critical infrastructure that is still used in White House memorandums, directives, and executive orders and in legislation.[3] This definition considers critical infrastructure to be "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Prior administrations issued memorandums shaping the national approach to critical infrastructure security, as shown in Figure 1. On February 12, 2013, Presidential Policy Directive 21, or PPD-21, *Critical Infrastructure Security and Resilience,* was issued. PPD-21 acknowledged the complexity of the nation's critical infrastructure and affirmed that it is the policy of the United States to strengthen critical infrastructure security and resilience against both physical and cyber threats. PPD-21 identified 16 critical infrastructure sectors and designated the EPA as the agency responsible for the water and wastewater systems sector. In this role, the EPA's responsibilities include providing institutional knowledge and specialized expertise for leading, facilitating, or supporting security and resilience programs within the water and wastewater systems critical infrastructure sector.

On April 30, 2024, PPD-21 was replaced with National Security Memorandum 22, or NSM-22, *Critical Infrastructure Security and Resilience*, which further affirmed that it is the policy of the United States to strengthen the security and resilience of its critical infrastructure. NSM-22 retained the 16 critical infrastructure sectors in PPD-21, along with the responsible agencies to protect the critical infrastructure against all threats and hazards. In doing so, NSM-22 again designated the EPA as the sector risk management agency for water and wastewater systems, maintaining the Agency's responsibilities as a source of institutional knowledge and specialized expertise.

Figure 1: Key water infrastructure-related milestones



Source: OIG analysis of key water infrastructure-related milestones. (EPA OIG image)

According to NSM-22, it is the objective of the United States to leverage federal agreements, such as grants and loans, to require or encourage owners and operators of critical infrastructure to meet or

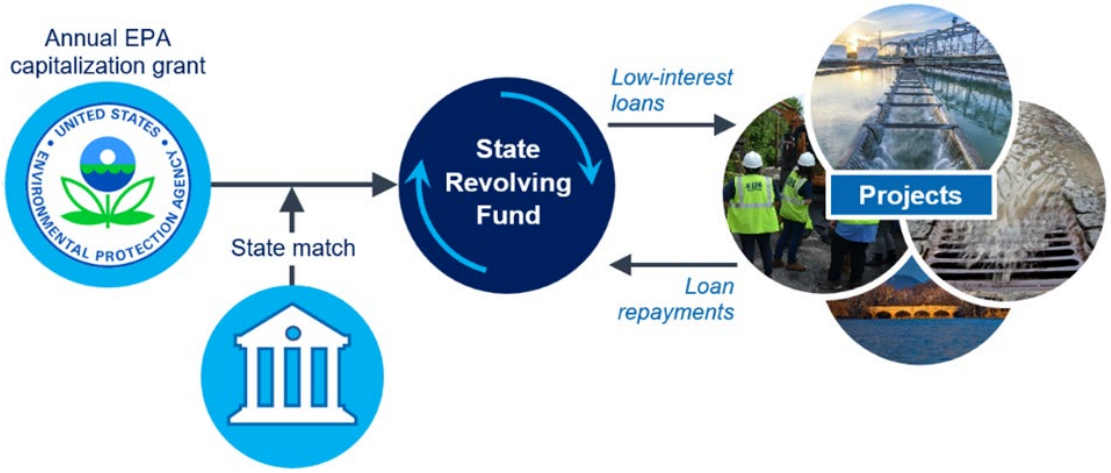
[3] 42 U.S.C. § 5195c(e).

exceed minimum security and resilience requirements. The EPA oversees billions of dollars in grants and loans for water and wastewater systems annually, and these funds can be used for projects that address risks or make infrastructure more resilient. For example, risk and resilience assessments and emergency response plans are eligible for funding through the EPA's DWSRF Program, which we describe below. Section 1433 of the Safe Drinking Water Act requires community water systems serving more than 3,300 persons to regularly develop or update risk and resilience assessments and emergency response plans.[4] The law specifies which topics the assessments and emergency response plans must address, including the risk from malevolent acts and natural hazards and the security and resilience of pipes, storage, computer systems, and other systems. Like other physical security or cybersecurity projects, assessments and plans must be included in state intended use plans, or IUPs, which we also discuss below, to receive DWSRF Program funds.

The Drinking Water State Revolving Fund Program

In 1996, Congress amended the Safe Drinking Water Act to establish the DWSRF Program, a financial assistance program that helps states finance critical water infrastructure projects that further the health protection objectives of the Safe Drinking Water Act. Congress annually appropriates funding for the EPA-administered DWSRF Program. The EPA makes DWSRF capitalization grants available to all 50 states and the Commonwealth of Puerto Rico based on need.[5] The state DWSRF functions as a state-based loan program for water systems, with the state required to match up to 20 percent of the entire capitalization grant. State revolving funds, or SRFs, including the DWSRF, provide low-cost financing for water systems and water infrastructure projects across the United States. As water systems repay their loans, the repayments and interest replenish the revolving fund to cover the state's future eligible infrastructure projects. Figure 2 illustrates the flow of funds in a state's DWSRF.

Figure 2: General steps in the DWSRF capitalization grant funding cycle



Source: OIG analysis of the *Drinking Water State Revolving Fund: Program Operations Manual, Provisional Edition*. (EPA OIG image)

[4] 42 § U.S.C. 300i-2.

[5] The EPA works with states and community water systems every four years to estimate DWSRF-eligible needs through the Drinking Water Infrastructure Needs Survey and Assessment.

The DWSRF Program funds a wide range of drinking water infrastructure projects, including the purchase of supervisory control and data acquisition, or SCADA, systems;[6] standby power generators; and the installation of security safeguards, such as fencing, gates, and cameras, to protect infrastructure and prevent vandalism or purposeful contamination of drinking water. State DWSRF programs can use funds for operator certification, source water protection, small system assistance, and public water system supervision. State DWSRF programs can use up to 31 percent of their capitalization grant to administer the program; these funds are known as set-asides. These set-asides can be used to fund state programs, technical assistance and training, and other activities that support public health protection. According to the EPA's *Supporting Cybersecurity Measures with the Drinking Water State Revolving Fund* fact sheet, issued in October 2019, conducting security assessments, including physical infrastructure and cybersecurity assessments, is an example of an eligible set-aside activity.

Each state must annually prepare an IUP that identifies how the intended uses of the requested federal funds support the goals of the state DWSRF program. The IUP must include, but is not limited to, a description of the state DWSRF program's long- and short-term goals and objectives for achieving the Safe Drinking Water Act's health protection objectives; a list of projects and eligible activities that the state intends to fund; and the criteria and method for distributing funds, referred to throughout this report as the ranking criteria.[7] Additionally, the information in the IUP must be provided in a format and manner that is consistent with the needs of the EPA regional administrator.

The EPA reviews state IUPs to ensure compliance with statutory and regulatory requirements related to the state DWSRF program. In the IUPs, the project descriptions reflect the priorities of individual water systems,[8] whereas the ranking criteria and set-asides reflect the state's priorities. Additionally, the Office of Water maintains a database for the SRFs with information about SRF-funded projects. This is known as the Office of Water State Revolving Fund, or OWSRF, database. While the IUPs describe the intended uses of funds, the OWSRF database collects information about initiated projects, such as project descriptions, cost information, and status updates. States are required to enter timely and accurate information into the database.

The Infrastructure Investment and Jobs Act

The IIJA includes $50 billion intended to strengthen water infrastructure, with 85 percent of that funding provided through the SRFs. It is the single largest investment in safe, clean drinking water ever made by the federal government. As such, an effective internal control system is particularly important. According to the GAO *Standards for Internal Control in the Federal Government*, commonly known as

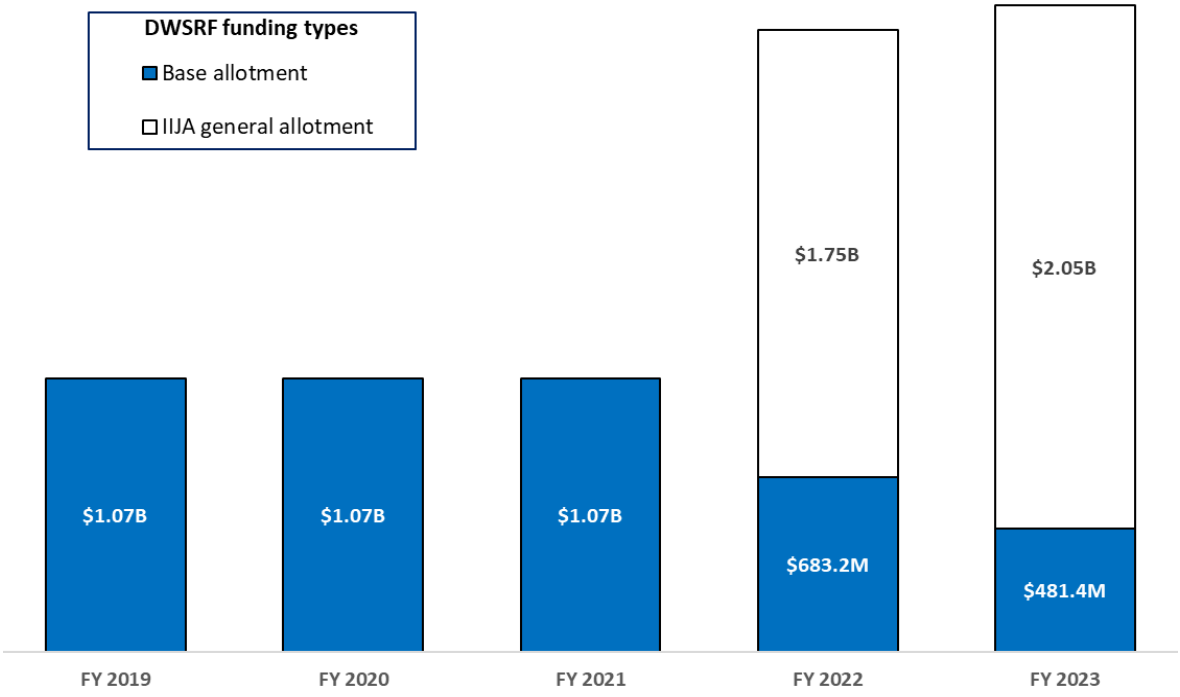
[6] SCADA systems can be used to remotely control and monitor the condition of assets, such as pump stations, valves, and wells, from a central location, enabling improved efficiency through real-time monitoring of all water activity within a water system's boundaries.
[7] 40 C.F.R. § 35.3555.
[8] A description of the project is a requirement in an IUP, but the level of detail is not prescribed and can vary by state.

the Green Book, an effective internal control system provides reasonable assurance that the organization will achieve its objectives.

Of the $50 billion for water infrastructure, the IIJA allocated $11.71 billion to the DWSRF Program to provide communities with general supplemental capitalization grants for a wide range of water quality infrastructure projects. Of this $11.71 billion, the IIJA allocated $3.8 billion to DWSRF general supplemental capitalization grants in fiscal year 2022 and FY 2023, specifically $1.75 billion in FY 2022 and $2.05 billion in FY 2023. Figure 3 summarizes federal DWSRF allotments for FYs 2019 through 2023.

In the March 2022 *Implementation of the Clean Water and Drinking Water State Revolving Fund Provisions of the Bipartisan Infrastructure Law* memorandum, the then-EPA assistant administrator for Water urged states to use the significant increase in SRF funding from the IIJA to foster water system resilience to all threats and hazards.[9] This funding can be used by public, private, and nonprofit drinking water utilities to conduct cybersecurity assessments and training, install equipment, or construct security safeguards to protect infrastructure. The IIJA allowed for states to make a reduced match of 10 percent on the general supplemental capitalization grants in FY 2022 and FY 2023 but returned to the 20 percent match requirement for subsequent years.

Figure 3: Federal DWSRF allotments for the 50 states and Puerto Rico, FY 2019–FY 2023



Source: OIG analysis of the DWSRF allotments. (EPA OIG image)

Notes: B = billion. M = million.

[9] EPA, Implementation of the Clean Water and Drinking Water State Revolving Fund Provisions of the Bipartisan Infrastructure Law (2022). The EPA has used the term "Bipartisan Infrastructure Law" interchangeably with the Infrastructure Investment and Jobs Act.

Responsible Offices

The Office of Water oversees implementation of the Safe Drinking Water Act. The Office of Water works with the ten EPA regional offices; other federal agencies; state, local, and tribal governments; the regulated community; the public; and other stakeholders. The Office of Water provides guidance, specifies scientific methods and data collection requirements, performs oversight, and facilitates communication among those involved in ensuring safe drinking water. Within the Office of Water, the Office of Ground Water and Drinking Water oversees the DWSRF Program. The final budget authority for the DWSRF Program was $638.3 million for FY 2022 and $504.8 million for FY 2023.[10]

Scope and Methodology

We conducted this evaluation from July 2024 to October 2025 in accordance with the *Quality Standards for Inspection and Evaluation* published in December 2020 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we perform the evaluation to obtain sufficient and appropriate evidence to support our findings.

We reviewed the 51 state DWSRF programs' IUPs that were used to apply for federal FY 2022 and FY 2023 DWSRF IIJA general supplemental capitalization grants.[11] Although similar security concerns exist for the Clean Water State Revolving Fund programs, we focused on the DWSRF programs.

To understand the DWSRF Program and its operations, we reviewed (1) relevant federal statutes and regulations, executive orders, and presidential directives; (2) the EPA's policies and guidance related to the DWSRF Program and the administration of IIJA funds, including memorandums and associated checklists regarding how the EPA regions interact with the states during IUP development and how the regions review the state-submitted IUPs; and (3) the EPA, Cybersecurity and Infrastructure Security Agency, and Federal Bureau of Investigation's jointly authored *Top Cyber Actions for Securing Water Systems* fact sheet.

To determine the extent to which IIJA funds are used to improve physical and cyber safeguards, including performing risk and resilience assessments, we analyzed EPA-approved, state-developed DWSRF IUPs associated with DWSRF IIJA general supplemental capitalization grants from FY 2022 and FY 2023. Because states describe their intended use of IIJA funds in their IUPs, we identified which plans mentioned physical security, cybersecurity, or related resilience efforts by measuring the use of 11 keywords: security, cyber, computer, network, SCADA, controller, access, data, vulnerability, threat, and emergency.[12] A state's inclusion of one or more keywords in its IUP served as an indication that the state might intend to use IIJA funds for projects that improve physical and cyber safeguards. We worked with the Office of Water to identify these keywords, as well as instances in which these

[10] The final DWSRF budget authorities for FY 2022 and FY 2023 were reported in the EPA's FY 2024 and FY 2025 Justification of Appropriation Estimates for the Committee on Appropriations, respectively.
[11] The 51 DWSRFs include the 50 states and the Commonwealth of Puerto Rico.
[12] Our use of SCADA as a keyword may have resulted in identifying the physical components of a project as opposed to statutory outcomes a state would like to achieve, thus limiting its frequency in ranking criteria or set-asides.

keywords may be used in an IUP but would not be indicative of an effort to improve physical security or cybersecurity. For example, we determined that, in an IUP, discussions about financial security were not an indication of an effort to improve physical security or cybersecurity, even though security was a keyword. When a keyword was used in a way that did not indicate plans to improve resilience, we considered the use to not be applicable to our review. Appendix A includes additional information about our methodology, as well as the detailed results of our review.

In addition, we reviewed the EPA's OWSRF database assistance agreement report to identify the number and extent of IIJA-funded projects to improve physical and cyber safeguards, including performing risk and resilience assessments, by measuring the use of keywords in the project descriptions of initiated projects. Further, we reviewed the GAO Green Book, and we interviewed DWSRF managers and staff within the Office of Water and DWSRF personnel within Region 5 to gain an understanding of the IUP approval process.

Limitations

We could not fully evaluate six IUPs. Because of the inherent flexibilities that states have in developing their IUPs, two states included project priority lists, a required element of an IUP, as a link that went to an external source. These links went to the project priority list for the current year, not the requested years. Consequently, we included these four provided IUPs in our analysis but could not determine the frequency of keywords in the four missing project priority lists. Accordingly, it is impossible to determine how the frequency of keywords may have changed if the missing IUP elements were available. Additionally, the EPA was not able to provide two finalized IUPs for FY 2023 during our data collection phase. These IUPs were not included in our analysis.

Prior Reports

We identified seven prior oversight reports related to the EPA's role in securing water systems. See Appendix B for more details.

Chapter 2
The EPA Could Improve Its Oversight of IIJA-Funded Projects That Intend to Address Physical and Cyber Resilience

The EPA has opportunities to improve its oversight of physical or cyber resilience projects. Such oversight would help the Agency meet and track strategic goals and requirements to safeguard water and wastewater critical infrastructure. In March 2022, the EPA urged, but did not require, states to fund projects that foster resilience to all threats and hazards, including cyberattacks.[13] The EPA confirmed during our fieldwork that projects that intend to improve physical security or cybersecurity cannot be identified unless a state includes relevant information about the project in its IUP or in the OWSRF database. Including this information in the IUP is voluntary, not a requirement. And although states are required to indicate in the OWSRF database whether a project addresses certain types of resilience, including cybersecurity resilience, the database does not allow states to specify whether the project addresses resilience to physical security threats and hazards. Adapting these reporting requirements would help the effectiveness of the Agency's oversight.

In the IUPs from FYs 2022 and 2023 that we analyzed, we identified projects and efforts to improve resilience to physical and cyber threats and hazards. However, we could not identify the extent to which states intended to use IIJA funds for these purposes because the EPA does not require the states to specify whether IIJA-funded projects address physical and cyber threats and hazards. Separately, through our analysis of the OWSRF database assistance agreement report, we identified 283 projects that received FY 2022 DWSRF IIJA general supplemental funding. Of these 283 projects, we identified four project descriptions that used the keyword security to indicate efforts to foster water system resilience to physical security threats. This shows that states generally did not describe such efforts in the OWSRF database.

Because IUPs are the mechanism that states use to prioritize the use of DWSRF funds, the absence of state IUP ranking criteria or set-aside descriptions that focused on resilience to physical and cyber threats and hazards indicates that security-focused projects may not be a priority for the state DWSRFs.[14] Similarly, the absence of expected keywords in IUP project descriptions may indicate that security-focused projects are not a priority for local water districts. Ultimately, IUPs and OWSRF database project descriptions that do not describe efforts to foster water system resilience to physical and cyber threats indicate that the $3.8 billion in IIJA funds allocated to DWSRFs in FYs 2022 and 2023 may not be prioritized for resilience improvements.

[13] EPA, Implementation of the Clean Water and Drinking Water State Revolving Fund Provisions of the Bipartisan Infrastructure Law (2022).

[14] From our review of the IUPs, we were not able to determine whether such resilience efforts are occurring but are not being described with the expected keywords or whether they are not occurring and thus are not being described.

The EPA Has Opportunities to Improve Its Oversight of Physical and Cyber Resilience Projects

The EPA does not have a specific method to identify and track projects that intend to address physical or cyber resilience. The Office of Ground Water and Drinking Water staff we interviewed explained that, in the OWSRF database, states are required to indicate whether projects address resilience, including cybersecurity resilience, but physical security resilience is not among the resilience types that the database tracks.[15] Separately, as of December 2025, there was no mechanism to query the OWSRF database for projects that aim to improve resilience to cyber threats and hazards. Additionally, in IUPs, including information that can be used to identify projects that address physical or cyber resilience is voluntary, not a requirement. Thus, projects that intend to improve resilience to physical and cyber threats and hazards cannot be identified in IUPs unless states decide to include relevant information. While some states include such information in IUP project descriptions or ranking criteria, other states do not. As a result, some IUPs are suitable for identifying or tracking physical security or cybersecurity projects, but other IUPs are not.

According to the GAO Green Book, an effective internal control system provides reasonable assurance that the organization will achieve its objectives. If project descriptions, rankings, or other information were consistent across IUPs, the EPA could leverage the IUPs as an oversight tool as part of an effective internal control system supporting Agency objectives to safeguard water and wastewater critical infrastructure. The EPA has the authority to add requirements to IUPs because federal regulations require that information in the IUP be provided in a format and manner that is consistent with the EPA regional administrator's needs. Because states must submit IUPs and some states already provide the relevant project details, the EPA is well postured to create such an internal control system. In doing so, the EPA would be better prepared to meet its strategic goals and requirements as the designated sector risk management agency for water and wastewater systems, as well as the Safe Drinking Water Act and NSM-22 requirements for ensuring resilience against threats and hazards to water and wastewater infrastructure.

Tracking projects that intend to improve physical or cyber resilience would allow the EPA to monitor state efforts to improve water system security and resilience. It would also allow the EPA to determine the extent to which DWSRF IIJA supplemental funds are used for projects that improve resilience to physical and cyber threats and hazards. Without a tracking method, the EPA cannot effectively oversee its progress in meeting its strategic goals and requirements to safeguard water and wastewater critical infrastructure.

Because the EPA does not have a specific method to identify projects that intend to address physical or cyber resilience, we considered the inclusion of keywords in the IUP as an indication that the state intends to use IIJA funds for projects that improve physical and cyber safeguards. Similarly, we

[15] Since July 2023, the OWSRF database has included a data field for states to use to select initiated projects that intend to address resilience, including cybersecurity resilience. However, as of December 2025, the database did not have an option to track projects with a physical security resilience element.

considered the inclusion of keywords in the OWSRF database as an indication that the state is using IIJA funds for projects that improve physical and cyber safeguards. Our review of keywords that were used in the IUPs and the OWSRF database, which we discuss in the sections below, provides a baseline of the projects that intend to address or are addressing physical or cyber resilience.

Some State IUPs Included Descriptions of Projects and Efforts to Improve Resilience to Physical and Cyber Threats and Hazards

By searching for keywords in the IUPs, we found descriptions of projects and efforts to improve resilience to physical and cyber threats and hazards. While we were able to identify projects and efforts to improve resilience by searching for keywords, we could not identify the extent to which states intended to use IIJA funds for these purposes because states are not required to include this information in their IUPs. Through our review, we could not determine whether the states that did not include keywords in their IUPs also did not prioritize efforts to improve resilience or whether they simply did not document their efforts to improve resilience using the keywords. Below we describe the resilience efforts we identified by searching the IUPs for the keywords security, cyber, and SCADA.

Some States Used the Keyword Security in Ways That Indicated Plans to Improve Resilience to Threats

By searching for the keyword security in the FY 2022 and FY 2023 IUPs that states used to apply for DWSRF IIJA general supplemental funds, we found descriptions of projects and efforts to improve resilience to physical and cyber threats. Specifically, in the IUPs that were used to apply for FY 2022 DWSRF IIJA general supplemental funds, 37 percent included the keyword security in their ranking criteria or set-aside descriptions in a way that indicated that the state intended to prioritize the use of funds to foster water system resilience to security threats and hazards, as shown in Table 1. For example, both Missouri and Colorado used security in their FY 2022 ranking criteria or set-aside descriptions. Missouri used the keyword security as a ranking criterion in its FY 2022 IUP, assigning ten points "for eligible security measures, including vulnerability assessments, emergency response plans, fencing, security cameras, and lights, motion detectors, secure chemical and fuel storage, security hatches and access panels, cross-connection control, and SCADA." This indicates that Missouri intends to prioritize projects with security measures. Colorado used the keyword security in a set-aside description in its FY 2022 IUP, which described that the state would "[c]ontinue to foster partnerships through Colorado's water/wastewater agency response network and national incident management system initiative to promote security and all-hazards preparedness throughout the state's drinking water community."

The use of the keyword security in ranking criteria or set-aside descriptions in a way that indicated that the state intended to improve resilience increased to 41 percent for the FY 2023 IUPs. In Maine's FY 2023 IUP, the state designated part of its $500,000 base and IIJA capitalization grant set-aside allotment for a new water system asset security grant "for eligible [Public Water Systems] to plan and/or implement security measures to protect water system assets. Activities eligible for the security measures may include fencing, signs, cameras, alarm systems." The examples from the FY 2022 and

FY 2023 IUPs illustrate how the use of the keyword security in an IUP's ranking criteria or set-aside description enabled us to identify projects and efforts to foster water system resilience to security threats and hazards.

Table 1: Use of the keyword security in state IUP ranking criteria or set-aside descriptions that indicate plans to improve resilience to threats

State IUPs that:	FY 2022 (%)	FY 2023 (%)
Used the keyword security in ranking criteria or set-aside descriptions to indicate plans to improve resilience	37	41
Did not use the keyword security in ranking criteria or set-aside descriptions to indicate plans to improve resilience	63	55
Were not available for evaluation	0	4

Source: OIG analysis of the EPA-approved state IUPs. (EPA OIG table)

Note: The FY 2023 Puerto Rico and Vermont IUPs were not available for evaluation.

Similar to the use of security in ranking criteria and set-aside descriptions, we identified state IUPs that used the keyword security in project descriptions. In the IUPs that states used to apply for FY 2022 DWSRF IIJA general supplemental funds, 25 percent of states included the keyword security in a project description to indicate the intended use of funds to foster water system resilience to security threats and hazards. For example, the FY 2022 Georgia IUP used the keyword in a project description that stated, "Numerous SCADA upgrades at 7 elevated water tank and 4 deep well locations to enhance system security and metering infrastructure are also to be installed." The percentage of IUPs that used the keyword security in project descriptions in ways that indicated plans to improve resilience increased to 35 percent in FY 2023, as shown in Table 2.

Table 2: Use of the keyword security in state IUP project descriptions that indicate plans to improve resilience to threats

State IUPs that:	FY 2022 (%)	FY 2023 (%)
Used the keyword security in project descriptions to indicate plans to improve resilience	25	35
Did not use the keyword security in project descriptions to indicate plans to improve resilience	75	61
Were not available for evaluation	0	4

Source: OIG analysis of the EPA-approved state IUPs. (EPA OIG table)

Note: The FY 2023 Puerto Rico and Vermont IUPs were not available for evaluation.

While we identified projects and efforts to improve resilience to physical and cyber threats by searching IUPs for the keyword security, from the IUPs, we could not determine the extent to which states intended to use IIJA funds to improve resilience to physical security and cybersecurity threats and hazards. In fact, more than 50 percent of the state IUPs we reviewed did not include the keyword security in a way that described a project or effort to improve resilience to physical and cyber threats.

Some States Used the Keyword Cyber in Ways That Indicated Plans to Improve Resilience to Threats

By searching for the keyword cyber in the FY 2022 and FY 2023 IUPs that states used to apply for DWSRF IIJA general supplemental funds, we identified IUPs with descriptions of projects and efforts to improve resilience to physical and cyber threats. Specifically, in the IUPs that were used to apply for FY 2022 DWSRF IIJA general supplemental funds, 18 percent of states included the keyword cyber in their ranking criteria or set-aside descriptions in a way that indicated plans to improve resilience. For example, the FY 2022 IUP for New Jersey included cyber in its description of ranking criteria, giving 45 points for project elements that include the "[a]ddition or enhancement of security measures at drinking water facilities, including but not limited to … cybersecurity, and auxiliary power sources." The percentage increased to 29 percent of states for FY 2023, as shown in Table 3. While some states, like New Jersey, used the keyword cyber in their IUP's ranking criteria and set-aside descriptions in ways that indicate plans to foster water system resilience to cyber threats and hazards, more than 65 percent of state IUPs did not use the keyword cyber in this way.

Table 3: Use of the keyword cyber in state IUP ranking criteria or set-aside descriptions that indicate plans to improve resilience to threats

State IUPs that:	FY 2022 (%)	FY 2023 (%)
Used the keyword cyber in ranking criteria or set-aside descriptions to indicate plans to improve resilience	18	29
Did not use the keyword cyber in ranking criteria or set-aside descriptions to indicate plans to improve resilience	82	67
Were not available for evaluation	0	4

Source: OIG analysis of the EPA-approved state IUPs. (EPA OIG table)

Note: The FY 2023 Puerto Rico and Vermont IUPs were not available for evaluation.

Similar to their use of the keyword cyber in ranking criteria and set-asides, some IUPs used the keyword cyber in project descriptions. In the IUPs that states used to apply for FY 2022 DWSRF IIJA general supplemental funds, 10 percent of states included the keyword cyber in a project description in a way that indicated plans to foster water system resilience to all threats and hazards. For example, Alabama used the keyword cyber in a project description for its FY 2022 IUP, which states, "FS010096-08 Mobile Board of Water & Sewer Commissioners (MAWSS) – Mobile DWSRF Master Plan Phase I (2019-2023) Supplemental … **cyber**security program design" (emphasis added). The percentage of IUP project descriptions that used the keyword cyber in ways that indicated plans to improve resilience dropped to 8 percent for FY 2023, as shown in Table 4.

Table 4: Use of the keyword cyber in state IUP project descriptions that indicate plans to improve resilience to threats

State IUPs that:	FY 2022 (%)	FY 2023 (%)
Used the keyword cyber in project descriptions to indicate plans to improve resilience	10	8
Did not use the keyword cyber in project descriptions to indicate plans to improve resilience	90	88
Were not available for evaluation	0	4

Source: OIG analysis of the EPA-approved state IUPs. (EPA OIG table)

Note: The FY 2023 Puerto Rico and Vermont IUPs were not available for evaluation.

While we identified projects and efforts to improve resilience to physical and cyber threats by searching IUPs for the keyword cyber, through the IUPs, we could not determine the extent to which states intended to use IIJA funds to improve resilience to physical security and cybersecurity threats and hazards. In fact, more than 65 percent of the state IUPs we reviewed did not include the keyword cyber in a way that described a project or effort to improve resilience to physical and cyber threats.

The Keyword SCADA Was Not Widely Used in Ranking Criteria and Set-Aside Descriptions, but It Was Widely Used in Project Descriptions

By searching for the keyword SCADA in the FY 2022 and FY 2023 IUPs that states used to apply for DWSRF IIJA general supplemental funds, we identified IUPs with descriptions of projects and efforts to improve resilience to physical and cyber threats. In the IUPs that were used to apply for FY 2022 DWSRF IIJA general supplemental funds, 10 percent of states included the keyword SCADA in their ranking criteria or set-aside descriptions in ways that indicated plans to improve resilience. For example, the FY 2022 IUP for Kentucky includes SCADA in the ranking criteria for approving projects, awarding 15 points for "[a]utomated and remote control systems (SCADA) that achieve substantial energy savings." The use of the keyword SCADA in this way indicates that the state intends to use funds to foster water system resilience. The percentage of IUPs with ranking criteria or set-aside descriptions that indicated plans to improve resilience increased to 14 percent for FY 2023, as shown in Table 5.

Table 5: Use of the keyword SCADA in state IUP ranking criteria or set-aside descriptions that indicate plans to improve resilience to threats

State IUPs that:	FY 2022 (%)	FY 2023 (%)
Used the keyword SCADA in ranking criteria or set-aside descriptions to indicate plans to improve resilience	10	14
Did not use the keyword SCADA in ranking criteria or set-aside descriptions to indicate plans to improve resilience	90	82
Were not available for evaluation	0	4

Source: OIG analysis of the EPA-approved state IUPs. (EPA OIG table)

Note: The FY 2023 Puerto Rico and Vermont IUPs were not available for evaluation.

States used the keyword SCADA widely in project descriptions. In the IUPs that states used to apply for FY 2022 DWSRF IIJA general supplemental funds, 63 percent of states included the keyword SCADA in a project description in a way that indicated plans to improve resilience. For example, Alabama used the keyword SCADA in a project description for its FY 2022 IUP, which described the "development of SCADA change management processes and procedures; design and implementation support of Wide Area Network (WAN) SCADA." The percentage of IUPs that included SCADA in a way that indicated plans to improve resilience increased to 65 percent for FY 2023, as shown in Table 6.

Table 6: Use of the keyword SCADA in state IUP project descriptions that indicate plans to improve resilience to threats

State IUPs that:	FY 2022 (%)	FY 2023 (%)
Used the keyword SCADA in project descriptions to indicate plans to improve resilience	63	65
Did not use the keyword SCADA in project descriptions to indicate plans to improve resilience	37	31
Were not available for evaluation	0	4

Source: OIG analysis of the EPA-approved state IUPs. (EPA OIG table)

Note: The FY 2023 Puerto Rico and Vermont IUPs were not available for evaluation.

While we identified projects and efforts to improve resilience to physical and cyber threats by searching IUPs for the keyword SCADA, through the IUPs, we could not determine the extent to which states intended to use IIJA funds to improve resilience to physical security and cybersecurity threats and hazards. For the IUPs that did not use the keyword SCADA, it is unknown whether SCADA-specific resilience efforts are occurring but are not being described, whether resilience efforts are occurring but not using SCADA, or whether such resilience efforts are not occurring and therefore are not being described in the IUPs.

SCADA investments without proper protocols could create vulnerabilities

According to a Cybersecurity and Infrastructure Security Agency news release, cyber actors obtained unauthorized access on February 5, 2021, to the SCADA system at a drinking water treatment facility. The Cybersecurity and Infrastructure Security Agency reported that the cyber actors likely accessed the system by exploiting cybersecurity weaknesses, including poor password security and an outdated operating system. This example highlights that investments in SCADA without proper cybersecurity protocols could create vulnerabilities at drinking water treatment facilities.

States Generally Did Not Use Keywords in Database Project Descriptions to Indicate Plans to Improve Resilience to Threats

While we identified projects to improve resilience to physical and cyber threats by searching the OWSRF database assistance agreement report for the keyword security, keyword use in database project descriptions was less frequent than in state IUPs. As discussed previously, states are responsible for entering information on initiated projects into the OWSRF database. We queried the EPA's OWSRF database assistance agreement report to identify the number and extent of state programs reportedly using IIJA funds to improve physical and cyber safeguards. Of the 283 projects identified in the OWSRF

database assistance agreement report as receiving FY 2022 IIJA general supplemental funding, we identified four projects, or 1.4 percent, that used the keyword security in the project description.

Of the four identified projects, the description for one project stated that the grantee requested "an emergency generator, security and lighting, and alarm systems for monitoring low pressure, power outages and security." The description for another project stated that "this project is addressing the serious signs of aging, deterioration, and deficiencies at the system's existing [reservoir]. Many portions of the reservoir are over 70 years old and in poor condition. The open-air reservoir is also particularly vulnerable to outside contaminants and security threats which can pose serious health risks to water customers. The proposed storage tank will improve the resilience and security of the existing system." These are both examples of how DWSRF IIJA funds are used to improve water system resilience. However, the limited number of project descriptions in the OWSRF database that used the word security indicates either that water systems are initiating projects that improve resilience but are not describing the projects using the keyword security or that water systems are not initiating such projects. As a result, we could not identify through our review the total amount of IIJA general supplemental funds being used to improve resilience to physical and cyber threats and hazards.

Conclusions

While the EPA urged states to use the significant increase in SRF funds from the IIJA to foster water system resilience to all threats and hazards, it did not require states to indicate in their IUPs whether projects intend to improve physical or cyber resilience. Therefore, it is difficult to determine from the IUPs the extent to which states intend to use DWSRF IIJA supplemental funds for projects that improve resilience to physical and cyber threats and hazards. Further, the varied use of resilience-related keywords in IUPs and OWSRF database project descriptions indicates that the EPA's urging of states to use SRF funds to foster water system resilience to all threats and hazards may not have resulted in states prioritizing the funds for such investments. Although our review of relevant keywords identified some projects and efforts to improve resilience to physical and cyber threats, neither we nor the EPA can accurately identify the total number of projects and efforts to do so, which means that the full amount of IIJA funds used for these purposes remains unknown. Ultimately, IUPs and OWSRF database project descriptions that do not describe efforts to foster water system resilience to physical and cyber threats indicate that the IIJA funds may not be prioritized for physical and cyber resilience improvements. Lack of investment in resilience projects leaves U.S. water systems at continued risk of physical and cyber threats and hazards. The EPA has opportunities to adapt its requirements so that it can improve its oversight of physical or cyber resilience projects. Such oversight would help the Agency meet and track strategic goals and requirements to safeguard water and wastewater critical infrastructure.

Recommendations

We recommend that the assistant administrator for Water:

1. Adopt a method for tracking Infrastructure Investment and Jobs Act-funded Drinking Water State Revolving Fund projects that intend to improve physical and cyber resilience against

threats to water critical infrastructure. Doing so could provide the Agency with an oversight tool to help meet and track strategic goals and requirements as the sector risk management agency.

2. Collaborate with state stakeholders to develop intended use plan guidance that helps states document their efforts to improve water system resilience to physical and cyber threats and hazards in project descriptions, rankings, and set-aside descriptions. Doing so would support a more effective internal control system and thereby provide reasonable assurance that the EPA will achieve its strategic goals and requirements to safeguard water and wastewater critical infrastructure.

Agency Response and OIG Assessment

The Agency's response to our draft report is in Appendix C. The EPA also provided technical comments, which we considered and incorporated as necessary.

The Agency agreed with our recommendations. For Recommendation 1, the Agency's proposed corrective actions partially meet the intent of the recommendation. The Agency asserted that it already developed a method for tracking IIJA-funded SRF projects that intend to improve physical and cyber resilience against threats to water critical infrastructure because the OWSRF database contains fields for data regarding resilience. Upon reviewing the OWSRF database with the Agency on December 11, 2025, we confirmed that the database contains a field asking whether a project has a resilience component. When a user indicates that a project includes a resilience component, the database prompts the user to select a subcategory. One of the subcategories is cybersecurity resilience. However, as of December 11, 2025, the database did not have an option for physical security resilience. In addition, the Agency did not have a mechanism to query the resilience subcategory data field. Therefore, unless the Agency modifies the OWSRF database, it cannot rely on the database as an oversight tool to help the Agency meet and track strategic goals and requirements related to physical resilience against threats to water infrastructure. Separately, the Agency did not have a mechanism to track a state's use of set-asides to promote physical or cybersecurity resilience. The Agency's current system does not meet the full intent of our recommendation because it does not track physical security resilience efforts or similar efforts in state set-asides. Therefore, Recommendation 1, to adopt a method for tracking IIJA-funded DWSRF projects that intend to improve physical and cyber resilience against threats to water critical infrastructure, remains unresolved.

For Recommendation 2, the Agency provided acceptable planned corrective actions and estimated milestone dates. The Agency committed to continue collaborating with the states to encourage support of cybersecurity initiatives and continue sharing best practices related to the physical security and cybersecurity resilience of water systems. For example, the Agency addressed cybersecurity priorities in a recent white paper that it jointly developed with the states. We consider Recommendation 2 resolved with corrective actions pending.

Status of Recommendations

Rec. No.	Page No.	Recommendation	Status*	Action Official	Planned Completion Date
1	15	Adopt a method for tracking Infrastructure Investment and Jobs Act-funded Drinking Water State Revolving Fund projects that intend to improve physical and cyber resilience against threats to water critical infrastructure. Doing so could provide the Agency with an oversight tool to help meet and track strategic goals and requirements as the sector risk management agency.	U	Assistant Administrator for Water	—
2	16	Collaborate with state stakeholders to develop intended use plan guidance that helps states document their efforts to improve water system resilience to physical and cyber threats and hazards in project descriptions, rankings, and set-aside descriptions. Doing so would support a more effective internal control system and thereby provide reasonable assurance that the EPA will achieve its strategic goals and requirements to safeguard water and wastewater critical infrastructure.	R	Assistant Administrator for Water	6/30/26

* C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

Appendix A

Intended Use Plan Review Methodology

In addition to collaborating with the Office of Water to identify 11 keywords relevant to physical security, cybersecurity, or related resilience efforts, we identified when each of the 11 keywords were used in an IUP. States included the keywords in their IUPs in the following four main ways:

- **Project descriptions,** which provide specific details on planned projects. Including a keyword in a project description indicates active plans to address physical security, cybersecurity, or related resilience.
- **Ranking criteria,** which are the factors that a state uses to create its project priority list in each IUP. The EPA allows each state the flexibility to set its own criteria. Including a keyword in its ranking criteria indicates that the state is prioritizing projects that address physical security, cybersecurity, or related resilience.
- **Set-asides,** which are a portion of IIJA capitalization grants that a state can choose to allocate to support state DWSRF program activities, technical assistance and training, and other activities that support public health protection. Including a keyword in its set-aside descriptions indicates that the state is focusing its resources to address physical security, cybersecurity, or related resilience.
- **Out-of-scope uses**, meaning that the use of a keyword was not an indication of an effort to improve physical security, cybersecurity, or related resilience.

In Table A-1, we share examples of applicable and out-of-scope uses of the 11 keywords we searched for in the IUPs.

Table A-1: Examples of applicable and out-of-scope uses of the 11 keywords

Keyword	Example of the keyword used in a way that indicates physical security, cybersecurity, or related resilience efforts (applicable use)	Examples of the keyword used in a way that does not indicate physical security, cybersecurity, or related resilience efforts (out-of-scope use)
Security	This year we will begin a new Water System Asset Security Grant. This grant is for eligible P[ublic] W[ater] S[ystem] to plan and/or implement **security** measures to protect water system assets.	Each loan is evaluated, and **security** is required to ensure that loans will be repaid to the fund.

Keyword	Example of the keyword used in a way that indicates physical security, cybersecurity, or related resilience efforts (applicable use)	Examples of the keyword used in a way that does not indicate physical security, cybersecurity, or related resilience efforts (out-of-scope use)
Cyber	Project includes a cybersecurity improvement based on **cyber** assessment.	Public Review and Comment … Comment Line item 2.N, resiliency and critical system functions, applicants should be allowed to receive cumulative points if they satisfy more than one of these criteria. While some of these line items overlap, others are unrelated. For instance, applicants could be incentivized to only consider **cybersecurity** measures instead of the location within the floodplain because they will only receive one set of points under this line item.
Computer	Proposed project involves the construction of a new second water well at the Richard Well Field, two standby generators at booster station sites, and upgrade **computer** and P[rogrammable] L[ogic] C[ontrollers] controllers for SCADA systems.	Does the Applicant have a **computer** to read meters and bill customers? __ YES __ NO.
Network	[E]ncourage small water systems to form partnerships, initiate contract operation and maintenance agreements, and implement mutual-aid agreements as via the New York Water and Waste Water Agency Response **Network.**	Redevelop the open ditch **network**.
SCADA	Security - 10 points will be assigned for eligible security measures, including vulnerability assessments, emergency response plans, fencing, security cameras, and lights, motion detectors, secure chemical and fuel storage, security hatches and access panels, cross-connection control, and supervisory control and data acquisition (**SCADA**).	Definition - **SCADA** Supervisory control and data acquisition.
Controller	Project Description - ...and upgrade computer and P[rogrammable] L[ogic] **C[ontrollers]** controllers for SCADA systems.	Retrofit or replacement of existing landscape irrigation systems to more efficient landscape irrigation systems, including moisture and rain sensing **controllers**.
Access	Security - 10 points will be assigned for … security hatches and **access** panels, cross-connection control, and supervisory control and data acquisition (SCADA).	Beginning with the F[ederal] F[iscal] Y[ear] 2011 Capitalization Grant, FFATA ensures that the public can **access** information on all recipients through *https://www.usaspending.gov*.

Keyword	Example of the keyword used in a way that indicates physical security, cybersecurity, or related resilience efforts (applicable use)	Examples of the keyword used in a way that does not indicate physical security, cybersecurity, or related resilience efforts (out-of-scope use)
Data	Contracted Services - Development of training programs to support … staff and P[ublic] W[ater] S[ystem] in the proper submission of electronic **data**.	Project is physically located and benefits a community in a Maryland County (including Baltimore City) where the U.S. Census **data** shows a declining population.
Vulnerability	System **Vulnerability** Assessment.	Community in a county with a Social **Vulnerability** Index score indicating a high level of **vulnerability** per the Center for Disease Control and Prevention mapping.
Threat	P[ublic] W[ater] S[ystem] Security Grants… Eligible P[ublic] W[ater] S[ystem]s must…Have attended a workshop regarding potential biological, chemical, and terrorism **threats** that affect P[ublic] W[ater] S[ystem]; inadequately treated surface water, are given high scores.	Public Review and Comment … Comment: Line item 2.H.3, addressing an emerging compound without a maximum contaminant level (MCL), should be awarded more points, perhaps 20. Many emerging compounds will be without an MCL for some time but still pose a **threat** to water resources and human health. Therefore, projects addressing this issue should receive a substantial portion of the 35 total points available for the Project Benefits section.
Emergency	**Emergency** Preparedness and Security subsidized training and continued updating of P[ublic] W[ater] S[ystem] **emergency** response plans.	Section Header – **Emergency** Financing.

Source: OIG analysis of the EPA-approved state IUPs. (EPA OIG table)

Note: We used bold text to emphasize keyword use in the examples.

We recorded applicable uses of the keywords along with the document page number and a citation. This allowed a peer to review to ensure that the analyses were comparable between team members. In addition, this allowed the project manager to conduct a spot check to confirm the total count, the documentation of where the keyword was used in the IUP, and the IUP's reference of an IIJA funding source. We tallied the raw data using Excel formulas to eliminate hand-counting errors. We used further screening formulas to count individual state keyword use, the number of different keywords used, and the change over time. We searched each state IUP for the 11 keywords used either in a project description or as a ranking criteria or set-aside. Additionally, we determined whether a keyword use was or was not an applicable use, as described previously.

We found that 88 percent of the state IUPs used to apply for FY 2022 DWSRF IIJA general supplemental funds used at least one of the 11 keywords related to physical security, cybersecurity, or related resilience efforts. In our professional judgment, the three keywords we highlighted in the report were often associated with resilience efforts that were relevant to our objective. While we identified resilience efforts associated with each keyword, we chose to highlight the keywords security and cyber in the report because they resulted in relevant descriptions of projects and efforts specifically meant to

improve resilience to physical and cyber threats and hazards. We also highlighted the use of SCADA because SCADA systems can be used to remotely control and monitor the condition of assets, such as pump stations, valves, and wells, from a central location. These monitoring systems could be an investment used to alert operators to changes in system status that may indicate a breach in physical security or cybersecurity.

As shown in Table A-2, in the IUPs that the states used to apply for FY 2023 DWSRF IIJA general supplemental funds, the percentage of states that used at least one of the keywords remained constant at 88 percent. However, because there were only two fiscal years of IUPs available for the scope of our evaluation, with 4 percent of FY 2023 IUPs unavailable for review, we cannot make any overarching statements about trends in states' priorities or plans for using the DWSRF IIJA general supplemental funds for physical security, cybersecurity, or related resilience efforts.

Table A-2: Use of keywords in state IUP project descriptions that indicate plans to improve resilience to threats

State IUPs that:	FY 2022 (%)	FY 2023 (%)
Used any of the 11 keywords in ranking criteria, set-aside descriptions, or project descriptions to indicate plans to improve resilience	88	88
Did not use any of the 11 keywords in ranking criteria, set-aside descriptions, or project descriptions to indicate plans to improve resilience	12	8
Were not available for evaluation	0	4

Source: OIG analysis of the EPA-approved state IUPs. (EPA OIG table)

Note: The FY 2023 Puerto Rico and Vermont IUPs were not available for evaluation.

Appendix B

Prior Reports

EPA OIG Report No. 25-N-0004, *Cybersecurity Concerns Related to Drinking Water Systems*, issued November 13, 2024, described a passive cybersecurity assessment involving 1,062 U.S. drinking water systems that each serve 50,000 or more people. The OIG Office of Investigations found that 97 of the drinking water systems assessed had either critical or high-risk cybersecurity vulnerabilities and that an additional 211 drinking water systems had either medium- or low-risk vulnerabilities. The vulnerable systems served a total of 26.6 million and 82.7 million people, respectively. The report warned that exploitation of the cybersecurity vulnerabilities could result in service disruption or irreparable physical damage to drinking water infrastructure. The report also highlighted issues with reporting cybersecurity incidents to the EPA. Specifically, the Office of Investigations found that the EPA does not have its own cybersecurity incident reporting system, and the office was unable to find documented policies and procedures related to the EPA's coordination with the Cybersecurity and Infrastructure Security Agency and other key federal and state authorities.

In GAO Report No. GAO-24-106744, *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, issued August 1, 2024, the GAO found that the EPA assessed aspects of cybersecurity risk but did not conduct a comprehensive sector-wide risk assessment or develop and use a risk informed strategy to guide its actions. The GAO reported that, while national reporting requirements for cyber incidents are being developed, known incidents have disrupted water sector operations. For example, foreign hackers targeted multiple water systems in late 2023, and cyberattacks threaten public health, the environment, and other critical infrastructure sectors. The GAO recommended that the EPA assess sector risk, develop and implement a national cybersecurity strategy, and evaluate the sufficiency of its legal authorities to carry out its cybersecurity responsibilities and seek additional authority as necessary. The EPA concurred with the recommendations and said that it is taking corrective actions. The GAO closed two recommendations, and two others remain open as of July 22, 2025.

In EPA OIG Report No. 23-P-0003, *The EPA Met 2018 Water Security Requirements but Needs to Improve Oversight to Support Water System Compliance,* issued November 21, 2022*,* we found that the EPA met the requirements of section 2013 of the America's Water Infrastructure Act of 2018 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, but the America's Water Infrastructure Act-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. However, the EPA did not provide adequate oversight to ensure that water systems—particularly small water systems—complied with the America's Water Infrastructure Act 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 America's Water Infrastructure Act requirements and may not understand their vulnerability to malevolent acts. We made four recommendations, including that the EPA review risk and resilience assessments and emergency response plans to identify improvements. As of December 6, 2023, we considered all four recommendations resolved.

In GAO Report No. GAO-22-105103, *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance*, issued February 9, 2022, the GAO found that federal agencies with a lead role to assist and protect one or more of the nation's 16 critical infrastructures were referred to as sector risk management agencies. Three of the 16 sector risk management agencies, including the EPA, had determined the extent of their sector's adoption of the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*. In doing so, lead agencies took such actions as developing sector surveys and conducting technical assessments mapped to framework elements. The sector risk management agencies for four sectors had taken initial steps to determine adoption. However, lead agencies for nine sectors had not taken steps to determine framework adoption. In prior reports, the GAO recommended that these nine sector risk management agencies (1) develop methods for determining the level and type of framework adoption by entities across their respective sectors and (2) collect and report sector-wide improvements. The GAO reported that most agencies have not yet implemented these recommendations from prior reports.

In GAO Report No. GAO-20-299, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, issued February 25, 2020, the GAO found that most of the nine agencies with a lead role in protecting the 16 critical infrastructure sectors had not developed methods to determine the level and type of adoption of the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*, as the GAO previously recommended. Specifically, two of the nine sector-specific agencies had developed methods, and two others had begun taking steps to do so. The remaining five sector-specific agencies did not yet have methods to determine framework adoption. Specifically, sector-specific agencies for 13 of the 16 sectors, including the EPA, noted that they had taken steps to encourage and facilitate use of the framework, such as developing implementation guidance that links existing sector cybersecurity tools, standards, and approaches to the framework. In addition, all 12 selected sector-specific agencies that the GAO interviewed described either fully or partially using the framework. Nevertheless, the GAO said that implementing its recommendations to the sector-specific agencies to determine the level and type of adoption remained essential to the success of protection efforts. Among these agencies, eight agreed with the recommendations, one neither agreed nor disagreed with the recommendations, and one partially agreed with the recommendations. The EPA concurred with its recommendation. As of July 22, 2025, eight of the recommendations are closed, including the recommendation to the EPA, and two are still open.

In GAO Report No. GAO-18-211, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, issued February 15, 2018, the GAO found that most of the 16 critical infrastructure sectors took action to facilitate adoption of the National Institute of

Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* by entities within their sectors. Federal policy directed nine sector-specific agencies, including the EPA, in consultation with the Department of Homeland Security and other agencies, to review the cybersecurity framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments. Among these agencies, five agreed with the recommendations, and four neither agreed nor disagreed with the recommendations. As of July 22, 2025, eight recommendations are closed, including the recommendation to the EPA, and one recommendation is open.

In EPA OIG Report No. 13-P-0349, *EPA Can Better Address Risks to the Security of the Nation's Drinking Water Through New Authorities, Plans, and Information*, issued August 21, 2013, we found that the EPA had implemented a number of activities to promote the security of drinking water systems. However, strategic planning and internal controls for the water security program needed to be strengthened to allow the Agency to measure the program's performance and progress in drinking water systems' preparedness, prevention, response, and recovery capabilities. We found that the EPA's strategic planning in this area was hampered by its limited authority over water security, the voluntary nature of its water security activities, and concerns related to protecting information. The report noted that these impediments could be overcome by the water security program using available data; using alternative methods to gather data; and seeking additional authority from Congress to collect, protect, and use information from water systems. The report also noted that the EPA should expand its internal controls to meet Federal Managers' Financial Integrity Act requirements. According to the EPA's Enterprise Audit Management System, as of September 2014, all corrective actions were completed.

Agency Response to the Draft Report

ASSISTANT ADMINISTRATOR FOR WATER

WASHINGTON, D.C. 20460

November 25, 2025

MEMORANDUM

SUBJECT: Response to the Office of Inspector General Draft Report, Project No. OSRE-FY24-0105, Evaluation of the Use of Infrastructure Investment and Jobs Act Funds for Drinking Water Security, dated October 10, 2025

FROM: Jessica L. Kramer Jessica Kramer Digitally signed by Jessica Kramer Date: 2025.11.25 13:48:54 -05'00'

TO: Nicole N. Murley, Acting Inspector General
Office of Inspector General

Thank you for the opportunity to review and respond to the Office of Inspector General's draft report titled, *Evaluation of the Use of Infrastructure Investment and Jobs Act Funds for Drinking Water Security Projects Project No. OSRE-FY24-0105*, dated October 10, 2025. The following is a summary of the U.S. Environmental Protection Agency's overall position, followed by its position on the draft report's recommendations.

AGENCY'S OVERALL POSITION

The EPA agrees with the OIG that without investments in resilience-related projects, United States water systems remain at risk from physical and cyber threats and hazards. Further, the EPA agrees that the state revolving funds have a role to play in ensuring physical and cybersecurity for these systems. With the rise of cyber threats to water systems, the EPA has coordinated with state SRF programs to discuss cybersecurity in the context of water infrastructure projects funded by the SRFs. Following the OIG's circulation of the draft report to the EPA, the agency, together with the states, released a white paper describing a variety of ways in which states can support SRF sub-recipients in integrating cybersecurity best practices, and provide guidance, resources, and support to SRF assistance recipients to reduce risks and enhance long-term reliability of the water sector.

As part of this project, the OIG performed keyword searches on state DWSRF 2022 and 2023 IIJA General Supplemental Intended Use Plans and projects in the OWSRF data system to assess the extent

to which states were prioritizing resiliency projects with a focus on physical and cyber security. The OIG recommends, first, that the EPA adopt a method for tracking projects that aim to improve resilience to physical and cyber threats; and, second, that the EPA collaborate with states on IUP-related guidance to ensure greater consistency in project ranking, project descriptions, and in descriptions of other resilience-related efforts. The EPA agrees with both Recommendation 1 and Recommendation 2 and provides additional context below.

In discussions with the OIG during its audit, the EPA cautioned that a keyword search methodology to identify physical and cybersecurity projects could be limiting. Resiliency-related project elements are most often part of a broader project primarily intended to address public health or other priorities (for example, upgrading a water treatment plant to meet a particular contaminant's Maximum Contaminant Level). Therefore resiliency, especially as only measured by a set of keywords, might not explicitly be included in project descriptions. This challenge of using key words is exacerbated because the description fields in both IUPs and the OWSRF data system are high-level summaries of the projects' overall purpose and, to the extent possible, major project elements. This is why the EPA developed a method for tracking IIJA-funded SRF projects, for both drinking water and wastewater programs, that intend to improve physical and cyber resilience against threats to water critical infrastructure. Since summer 2021, the agency updated the OWSRF data system to include a distinct and separate checkbox asking specifically about resiliency, including physical and cyber resiliency.

With respect to Recommendation 2 that seeks EPA collaboration with states on IUP-related guidance, the EPA has worked cooperatively with states to provide them with maximum flexibility in their IUPs, within the parameters of the law. More specifically, the Safe Drinking Water Act requires that states implement their SRFs consistent with three statutory priorities: to (1) address the most serious risk to human health; (2) fund projects that are necessary to ensure compliance with the drinking water regulations; and (3) to assist systems most in need on a per household basis according to State affordability criteria. (42 U.S.C. 300j-12(b)(3)(A)). That said, as noted above, the EPA has addressed cybersecurity priorities in a recent white paper jointly developed with states and will collaborate with states at upcoming meetings to address the OIG's findings and recommendations. The EPA will continue this collaboration with the cooperative-federalism foundation of SDWA that recognizes state expertise in understanding the unique water quality and public health challenges of their state and gives them the lead role in working with communities to address those challenges.

As an attachment to this response, the EPA is including technical comments that provide more specific feedback on the draft report**.**

AGENCY RESPONSE TO RECOMMENDATIONS

OIG Recommendation 1: Adopt a method for tracking Infrastructure Investment and Jobs Act-funded Drinking Water State Revolving Fund projects that intend to improve physical and cyber resilience against threats to water critical infrastructure. Doing so could provide the Agency with an oversight tool to help meet and track strategic goals and requirements as the sector risk management agency.

EPA Response to Recommendation 1 – Agree

During the OIG's audit, the EPA informed the OIG that fields in OWSRF data system is the method for tracking IIJA SRF projects related to physical and cyber resilience for both DWSRF and CWSRF programs. States are required to provide information on the resiliency features of projects through the OWSRF data system.

Proposed Corrective Action: As the agency has included since 2021, the EPA will continue to use existing physical and cyber resilience data fields in the OWSRF data system. This assists the agency in assessing the extent of funds going to physical or cyber resilience-focused projects or activities. The EPA will communicate with states to remind them of these data fields and to reinforce that states should use these fields even if only portions of projects address physical and cyber resilience.

Expected Date of Completion: June 30, 2026.

OIG Recommendation 2: Collaborate with state stakeholders to develop guidance for intended use plans to improve the consistency of project descriptions, rankings, or designations of efforts related to improve water system resilience to physical and cyber threats and hazards. Doing so would support a more effective internal control system and thereby provide reasonable assurance that the EPA will achieve its strategic goals and requirements to safeguard water and wastewater critical infrastructure.

EPA Response to Recommendation 2 – Agree

Cooperative federalism, one of the pillars of the DWSRF, calls for the agency to collaborate with states to ensure they are provided flexibilities that best support their state-specific needs. For instance, in October 2025, the EPA released a white paper drafted jointly with states describing a variety of ways in which states can support SRF sub-recipients in integrating cybersecurity best practices, and to provide guidance, resources, and support to SRF assistance recipients to reduce risks and enhance long-term reliability of the water sector. The EPA will continue to collaborate with states to encourage support of cybersecurity initiatives and has shared physical and cyber security best practices in support of efforts related to improving water system resilience. The agency has a cybersecurity fact sheet, white paper and a DWSRF physical security fact sheet.

Proposed Corrective Action: The EPA will collaborate with state stakeholders to develop guidance that aims to enhance the use of consistent terminologies for SRF projects improving water system resilience in IUPs, to reinforce the use of related data fields in OWSRF data systems, and to highlight state and EPA cybersecurity and resilience resources.

Expected Date of Completion: June 30, 2026.

If you have any questions regarding this response or the technical comments, please have your staff contact the Office of Water Audit Follow-Up Coordinator Carla Hagerman, at Hagerman.Carla@epa.gov.

Appendix D

Distribution

The Administrator
Deputy Administrator
Associate Deputy Administrator
Assistant Deputy Administrator
Chief of Staff, Office of the Administrator
Deputy Chief of Staff for Management, Office of the Administrator
Agency Audit Follow-Up Official
Chief Financial Officer and Chief Administrative Officer
Assistant Administrator for Water
Principal Deputy Assistant Administrator for Water
Agency Audit Liaison
Agency Audit Follow-Up Coordinators
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for External Affairs
Deputy Associate Administrator for Public Affairs, Office of External Affairs
Deputy Assistant Administrator for Management, Office of Water
Deputy Assistant Administrator for Regulatory and Scientific Affairs, Office of Water
Deputy Assistant Administrator for Strategic Initiatives, Office of Water
Chief of Staff, Office of Water
Director, Office of Program Analysis, Regulatory, and Management Support, Office of Water
Director, Office of Ground Water and Drinking Water, Office of Water
Associate Director, Office of Program Analysis, Regulatory, and Management Support, Office of Water
OIG Liaison, Office of Policy and Regulatory Management, Office of the Administrator
GAO Liaison, Office of Policy and Regulatory Management, Office of the Administrator
Audit Follow-Up Coordinators

Whistleblower Protection

U.S. Environmental Protection Agency

The whistleblower protection coordinator's role is to educate Agency employees about prohibitions against retaliation for protected disclosures and the rights and remedies against retaliation. For more information, please visit our website.

Contact us:

Congressional & Media Inquiries: OIG.PublicAffairs@epa.gov

EPA OIG Hotline: OIG.Hotline@epa.gov

Web: epa.gov/oig

Follow us:

X: @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @EPA_OIG

www.epa.gov/oig