OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

October 21, 2026

The Honorable Gary Palmer
Chairman
Subcommittee on Environment
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Palmer:

Enclosed please find my responses to the Questions for the Record that I received from Representative Laurel Lee following my appearance before the House Committee on Energy and Commerce, Subcommittee on Environment, on February 24, 2026.

Sincerely,

Nicole N. Murley
Deputy Inspector General performing
the duties of the Inspector General

cc: The Honorable Paul Tonko, Ranking Member, Subcommittee on Environment

Anyone with knowledge of potential fraud, waste, abuse, misconduct, or mismanagement should contact the OIG Hotline via OIG.Hotline@epa.gov, 888-546-8740, or our online form.

Responses to Questions for the Record from Representative Laurel Lee to
Deputy Inspector General Performing the Duties of the Inspector General Nicole Murley

1. **Hillsborough County residents expect that every federal dollar invested in water infrastructure is spent responsibly. Your office identified tens of millions of dollars in unknown or improper payments in the State Revolving Fund (SRF) programs. Can you explain in detail what breakdowns in internal controls led to these findings and what that means for taxpayer accountability?**

   Our January 2026 report identified several internal control breakdowns in the execution, documentation, reporting, and quality control of the EPA's SRF improper payment review process.

   First, we found that reviewers did not consistently follow the EPA's existing Transaction Testing Standard Operating Procedures and *SRF Annual Review Guidance* when reviewing transactions and preparing program evaluation reports. Reviewers did not always question payments for ineligible expenses or require adequate documentation to determine whether payments were allowable and properly supported. In some cases, reviewers accepted unapproved or unsigned construction invoices, summary information instead of underlying documentation, insufficient support for payroll and administrative expenses, and invoices for professional services that lacked detailed time sheets, hourly rates, or project-specific information.

   Second, we identified weaknesses in the controls for classifying and documenting the results of transaction testing. Under applicable payment integrity requirements, when documentation is insufficient to determine whether a payment is proper, the payment should be classified as "unknown" and, for reporting purposes, treated as improper. We found instances in which reviewers identified missing or insufficient documentation but failed to classify or report the payment accordingly. Some transaction testing worksheets also had incomplete required sections or lacked a clear determination of whether the payment was proper or improper.

   Third, controls did not consistently ensure that improper payments identified during testing were accurately carried through the reporting process. We found cases in which improper payments noted on worksheets were not reflected in the program evaluation report or reported to EPA headquarters. Reviewers also did not consistently report payments as improper when the underlying error had already been corrected. Likewise, negative cash draws, which may indicate that a state corrected a prior improper payment, were not consistently investigated, documented in program evaluation reports, or reported as required.

   Finally, we identified a quality control weakness; existing processes did not provide reasonable assurance that transaction testing was accurately executed and that the results were consistently and accurately reported across the transaction testing worksheets, program evaluation reports, and information submitted to EPA headquarters. We recommended that the

agency establish robust and enforceable controls for comprehensive quality reviews of transaction testing.

The EPA's proposed corrective actions directly addressed the control deficiencies we identified. The agency agreed to revise its Transaction Testing Standard Operating Procedures to more clearly specify the documentation required to justify payments; develop a training plan for transaction testers, EPA personnel, and states on the revised procedures and related internal control processes; and revise the standard operating procedure to delineate and document the components of the quality control process. The agency also agreed to update its payment integrity risk assessments for the Clean Water and Drinking Water SRF programs. Although the agency disagreed with our conclusion that unknown or improper payments were unreported, it accepted our recommendations and committed to improvements. In an April 27, 2026, memorandum, we determined that the EPA's planned actions met the intent of the three open recommendations, and we consider all recommendations resolved pending completion of the corrective actions. As a result, our audit directly led to increased oversight and accountability and better stewardship of taxpayer dollars.

a. **And what are some ways that Congress can strengthen oversight of these programs to ensure transparency further on down the road?**

   As we have previously noted, one of the best ways to maintain program effectiveness and integrity of oversight is to ensure that the SRFs are maintaining accurate and accessible documentation of how taxpayer dollars are spent. Accordingly, Congress may wish to consider requiring:

   - States to maintain SRF project documentation in a digital format that is accessible for oversight.
   - SRF data to be submitted to the EPA in a machine-readable and standardized format rather than via paper or scanned PDFs. States receiving capitalization grants should submit programmatic and financial data in machine-readable, standardized formats that enable aggregation, analysis, and public reporting.
   - The EPA to establish data validation standards before allocating federal infrastructure funds.

2. **In your testimony, you state that in 2024, you alerted the EPA to key cybersecurity vulnerabilities at large drinking water facilities serving millions of Americans and that if exploited, these vulnerabilities could degrade functionality, cause loss of service, or facilitate the theft of information. Without endangering operational security, could you go into more detail about the vulnerabilities large drinking water facilities have and how we can help harden them from cyber threats?**

We have identified water cybersecurity as a significant risk to public health and critical infrastructure for several years. The EPA needs to improve its overall oversight of water systems,

including ensuring compliance with water sector requirements and promoting the adoption of effective cyber and physical security controls.

The America's Water Infrastructure Act of 2018 amended the Safe Drinking Water Act, or SDWA, to require that drinking water systems serving more than 3,300 people assess their risk from malevolent acts, including cyberattacks, and natural hazards, and develop emergency response plans based on those assessments. However, in a November 2022 report, we described that the smallest water systems subject to these requirements—systems serving 3,301–49,999 people—were particularly likely to struggle to meet the requirements and that the EPA did not provide adequate oversight to ensure the water systems' compliance with the requirements. As a result of noncompliance, water system operators may not understand their system's vulnerability to malevolent acts, including cyberattacks.

In a November 2024 report, we alerted the agency to widespread cyber vulnerabilities across the nation's drinking water systems. As part of our oversight of the agency's role as the sector risk management agency, we conducted a passive cybersecurity assessment of 1,062 drinking water systems serving more than 193 million people. The scan reviewed more than 75,000 IP addresses and 14,400 domains, and we identified 97 systems, serving 26.6 million users, with critical or high-risk vulnerabilities that could be exploited to degrade functionality, deny service, or steal sensitive information. Another 211 systems, serving over 82 million people, exhibited medium or low-risk issues, such as externally visible open portals. Common problems included outdated software, poor IT hygiene, insecure email configurations, and signs of adversarial probing or malicious activity. If exploited, these exposures could cause severe operational disruptions or even permanent infrastructure damage. We also found that the EPA did not have its own cybersecurity incident reporting system for water systems and relied on the Cybersecurity and Infrastructure Security Agency and other partners for notifications. We also noted the absence of documented procedures describing how the EPA coordinates with federal, state, and local partners during cyber incidents.

These findings align with those from an August 2024 GAO report, which recommended that the agency develop a national water sector cybersecurity strategy, assess sector risk, and evaluate whether it needs additional authority. The findings also echo a May 2024 EPA enforcement alert that identified that water systems had inadequate risk and resilience assessments and emergency response plans. The alert also noted significant failures in best practices. For example, the alert explained that some water systems failed to change default passwords, used single logins for all staff, and failed to curtail former employee access.

A third OIG report, issued in May 2026, underscored that strengthening resilience is also a funding and oversight challenge. The evaluation reviewed state intended use plans and project descriptions associated with $3.8 billion in Infrastructure Investment and Jobs Act, or IIJA, Drinking Water State Revolving Fund grants. While some states described projects aimed at

improving physical or cyber resilience, most did not use terminology that clearly identified such efforts. Because the EPA does not require states to report cybersecurity-related project details in a consistent way, we could not determine the amount of IIJA funds being directed toward protecting water systems from physical and cyber threats. That lack of visibility limits the EPA's ability to track progress and ensure that funds are being prioritized where risk is greatest.

Although cyber threats to drinking water systems are serious and evolving, when utilities adopt recommended practices and take advantage of federal support, they substantially reduce risk and strengthen the resilience of systems that are essential to public health, economic stability, and national security. In the 2024 EPA enforcement alert, the EPA, the Cybersecurity and Infrastructure Security Agency, and the Federal Bureau of Investigation outlined clear, practical ways to help systems harden their defenses. Additionally, the EPA continues to expand support to the sector, offering technical assistance, tools, training, and funding to strengthen cybersecurity. Last year, the agency published new and updated planning tools that water systems across the country can use to help prevent and respond to cybersecurity incidents and announced grant funding to help mid-sized and large water systems strengthen their resilience against cyberattacks and extreme weather events.

However, while the EPA can oversee, assist, and encourage local cybersecurity efforts, the agency is limited in what it can require. An August 2026 Congressional Research Service report highlighted that recent cyberattacks on water systems have raised questions about the effectiveness of water systems' compliance with section 1433 of SDWA. The report also noted questions surrounding the EPA's use of its SDWA authorities to address cybersecurity. For example, in March 2023, the EPA issued an interpretive memorandum to require states, as a part of their SDWA primary enforcement responsibilities, to evaluate water system operational technology cybersecurity during triennial sanitary surveys. Stakeholders filed a petition for judicial review, arguing that the EPA did not follow the Administrative Procedure Act when issuing the memorandum and that the agency's expansion of the sanitary survey exceeded its statutory authority under SDWA. In October 2023, the EPA rescinded the interpretive memorandum and its requirements.

Ultimately, our oversight work, along with the other reports mentioned, paint a consistent picture. Significant cyber vulnerabilities exist across the water sector, including in large systems serving millions. Many vulnerabilities stem from basic cyber hygiene gaps, insufficient asset management, and outdated or incomplete risk and resilience assessments and emergency response plans. Funding intended to improve cyber and physical security cannot be tracked reliably without clear reporting requirements. The agency needs enhanced visibility, clearer authorities, and stronger coordination mechanisms to fully meet its responsibilities as the sector risk management agency. And because cybersecurity remains largely voluntary for water systems, cybersecurity improvement needs compete with other regulatory obligations while threat actors continue to evolve faster than many utilities can.

These issues underscore the importance of continued congressional oversight of cybersecurity efforts within the water sector, including ongoing examination of authorities, responsibilities, implementation challenges, and emerging risks. We believe that it will take the EPA working productively with the OIG, industry partners, and state and local governments to address this ever-growing issue, and that this is an important area for continued oversight. We are currently conducting an evaluation of the EPA's progress in fulfilling IIJA requirements related to water and wastewater system cybersecurity. We will share the results of that evaluation with the committee and with your office after we issue the final report.