# Prioritization Framework for Technical Cybersecurity Support to Public Water Systems – Report to Congress

Office of Water

EPA817-R-22-001

May 2022

## Contents

# EXECUTIVE SUMMARY

The Infrastructure Investment and Jobs Act (Public Law No. 117-58) requires the U.S. Environmental Protection Agency (EPA), in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), to develop a Prioritization Framework to identify public water systems (including sources of water for those public water systems) that, if degraded or rendered inoperable due to an incident, would lead to significant impacts on the health and safety of the public. EPA, in coordination with CISA, is to use the Prioritization Framework to develop a Technical Cybersecurity Support Plan for public water systems.

In developing the Prioritization Framework, EPA must incorporate consideration of four criteria: (1) whether cybersecurity vulnerabilities for a public water system have been identified under Section 1433 of the Safe Drinking Water Act (SDWA), (2) the capacity of a public water system to remediate a cybersecurity vulnerability without additional Federal support, (3) whether a public water system serves a defense installation or critical national security asset, and (4) whether a public water system, if degraded or rendered inoperable due to an incident, would cause a cascading failure of other critical infrastructure.

Finally, EPA must submit to the appropriate Congressional committees a report describing the Prioritization Framework not later than May 24, 2022. This report was prepared in fulfillment of this requirement.

The Prioritization Framework is structured as a series of qualitative questions stemming from the statutory criteria. This structure will provide EPA and CISA with the necessary flexibility to tailor the prioritization of water systems for technical cybersecurity support to specific circumstances and water system needs.

# STATUTORY REQUIREMENTS FOR THIS REPORT

The Infrastructure Investment and Jobs Act (the Act) became Public Law No. 117-58 on November 15, 2021. Section 50113 of the Act amends Part B of the SDWA (42 U.S.C. 300g et seq.) by adding at the end the following: Section 1420A. Cybersecurity Support for Public Water Systems.

Subsection (b)(1) of this section requires EPA, in coordination with CISA, to develop a Prioritization Framework within 180 days of the Act's enactment to identify public water systems (including sources of water for those public water systems) that, if degraded or rendered inoperable due to an incident, would lead to significant impacts on the health and safety of the public.

Subsection (b)(2) specifies that EPA, in coordination with CISA, is to use the Prioritization Framework to develop a Technical Cybersecurity Support Plan for public water systems within 270 days of the Act's enactment. In alignment with the deadlines specified in the statute, this report addresses the Prioritization Framework only. The Technical Cybersecurity Support Plan will be provided in a subsequent report.

In developing the Prioritization Framework, EPA must incorporate consideration of the following four criteria to the extent practicable (paragraph (b)(1)(B) of this subsection):

(1) whether cybersecurity vulnerabilities for a public water system have been identified under Section 1433 of the SDWA

- Note: SDWA Section 1433 requires community water systems serving over 3,300 people to develop a risk and resilience assessment, which must include electronic, computer, or other automated systems, and an emergency response plan that must include strategies and resources to improve…the cybersecurity of the system.

(2) the capacity of a public water system to remediate a cybersecurity vulnerability without additional Federal support,

(3) whether a public water system serves a defense installation or critical national security asset, and

(4) whether a public water system, if degraded or rendered inoperable due to an incident, would cause a cascading failure of other critical infrastructure.

Further, EPA must consult with such Federal or non-Federal entities as determined to be appropriate by the Administrator (paragraph (b)(3) of this subsection). To fulfill this requirement, EPA established a workgroup with the Water Sector Coordinating Council, Water Government Coordinating Council, and CISA (hereinafter, the workgroup). This workgroup held initial meetings to discuss proposed approaches to the Prioritization Framework and, subsequently, to review draft versions of this report.

Finally, EPA must submit to the appropriate Congressional committees a report describing the Prioritization Framework not later than 190 days after the date of enactment of the Act. Hence, the statutory due date for this Prioritization Framework report is May 24, 2022.

# CONSIDERATION OF THE NATIONAL CRITICAL INFRASTRUCTURE PRIORITIZATION PROGRAM

EPA and the workgroup considered whether existing prioritization criteria could fulfill the requirements of the Act. The Department of Homeland Security (DHS) maintains a classified list of critical infrastructure systems and assets that "would, if destroyed or disrupted, cause national or regional catastrophic effects." This list was developed and is maintained through the National Critical Infrastructure Prioritization Program (NCIPP).

Under the NCIPP, qualifying domestic infrastructure may be designated as Level 1 or 2 based on the projected impact of an adverse event, such as an industrial accident, natural disaster, or malicious act (e.g., cyber-attack). For all critical infrastructure sectors, including water but excluding food and agriculture, a facility or system is assigned as Level 1 or 2 if a disruption would result in at least two of the following consequences:

- Greater than 5,000 (Level 1) or 2,500 (Level 2) prompt fatalities,
- Greater than $75 billion (Level 1) or $25 billion (Level 2) in first-year economic consequences,
- Mass evacuations with a prolonged absence of greater than three months (Level 1) or 1 month (Level 2) and/or,
- Severe degradation of the Nation's national security capabilities, including intelligence and defense functions, but excluding military facilities.

Alternatively, a facility or system may be assigned to the list based on a first-year economic impact of $150 billion or more (Level 1) or at least $50 billion (Level 2). For water systems, contamination, intentional or otherwise, is not a permitted scenario.

The number of public water systems that meet these criteria and are designated as level 1 or 2 under the NCIPP is well below one percent of all water systems in the sector. Further, the NCIPP criteria have the effect of selecting the largest water systems, which typically have the most resources to address cybersecurity vulnerabilities. Consequently, the criteria for Level 1 and 2 facilities under the NCIPP would not be effective for the purposes of the Prioritization Framework under the Act, which is to prioritize technical cybersecurity support across the entire water sector. Accordingly, EPA did not use the NCIPP criteria in the Prioritization Framework

# POSSIBLE USE OF A PRIORITIZATION FRAMEWORK FOR TECHNICAL CYBERSECURITY SUPPORT

Both EPA and CISA currently offer ongoing technical cybersecurity support to public water systems through programs such as EPA's Cybersecurity Technical Assistance Provider Program and CISA's Cyber Hygiene Services. The Technical Cybersecurity Support Plan report, which EPA will develop pursuant to the Act following this report, will describe these programs in detail.

In addition, when a situation occurs that creates an elevated cyber risk level, such as knowledge of a significant cyber vulnerability or new cyber threat, EPA and CISA work with Federal and state government partners, WaterISAC, and water sector associations to assist water systems with undertaking mitigation actions. This assistance may comprise of alerts, webinars, and direct outreach to water systems.

Technical cybersecurity support from EPA and CISA is provided to water systems upon request. Receipt of this support by a water system is voluntary. To date, EPA and CISA have been able to provide requested technical cybersecurity support to water systems without delay. Consequently, a prioritization framework for delivering technical cybersecurity support to water systems has not factored into EPA or CISA's technical assistance efforts.

The Prioritization Framework described in this report could potentially be used under a scenario in which many water systems require technical cybersecurity support at the same time. Such a scenario might involve, for example, the discovery of a widespread zero-day vulnerability (i.e., a vulnerability in a system or device that has been disclosed but not yet patched) that impacts numerous water systems and that many water systems lack the technical capability to correct without assistance. If EPA or CISA were unable to assist all water systems that require help in a timely manner, then this Prioritization Framework could be employed to determine the order in which water systems receive support.

## PRIORITIZATION FRAMEWORK GOALS

Based on workgroup discussions, EPA identified several goals for the Prioritization Framework:

- **Flexible structure:** As discussed above, use of the Prioritization Framework may be most useful in circumstances resulting in requests for technical cybersecurity support that exceed the near-term capacity of EPA or CISA. Thus, the Prioritization Framework should be highly flexible so that EPA or CISA can tailor it to meet the risks and demands of exigent circumstances.
- **Allow consideration of individual water system circumstances:** Under the conditions where the Prioritization Framework might be used, the risks, capabilities, resources, needs, and other factors that impact the response of the water sector to the situation will vary widely among water systems. The Prioritization Framework should allow EPA or CISA to consider the circumstances of individual water systems.

- **Compatible with dynamic cybersecurity technical support capabilities of EPA and CISA:** The technical cybersecurity support that EPA and CISA offer to water systems will evolve in response to changing threat conditions, resources, and the requests of the water sector. Accordingly, the Prioritization Framework should accommodate the dynamic nature of EPA and CISA's capabilities.
- **Incorporate statutory criteria:** The Prioritization Framework should incorporate, to the extent practicable, the four criteria listed in the statute in a manner compatible with the other goals listed here. Consequently, the use of a particular criterion and the weight accorded to it in a prioritization scenario may vary based on the circumstances.
- **Environmental justice:** The Prioritization Framework should provide for fair treatment of all people regardless of race, color, national origin, or income, with respect to technical cybersecurity support.

## PRIORITIZATION FRAMEWORK

The Prioritization Framework is structured as a series of qualitative questions stemming from the statutory criteria. This qualitative structure will provide EPA and CISA with the necessary flexibility to tailor the prioritization of water systems for technical cybersecurity support to specific threat circumstances and water system needs.

The Framework is not designed to assign a water system to a fixed prioritization rank independent of a scenario where prioritization is needed. Rather, it reflects the understanding that decisions on prioritizing water systems for technical cybersecurity support would depend on the circumstances of a particular scenario (e.g., the type of cybersecurity vulnerability and technical support required, the number of water systems requesting assistance, and the capacity of EPA or CISA to deliver support).

As described above, existing circumstances have not required either EPA or CISA to use a prioritization framework for technical cybersecurity support to date. Should the need for a prioritization framework arise in the future, the Framework offered here could be adjusted as needed.

Under the Prioritization Framework, a water system requesting technical cybersecurity support during a surge scenario (i.e., a scenario where demand for technical cybersecurity support from EPA or CISA exceeds the near-term capacity of the Agency) would respond to the Framework questions. The Agency (EPA or CISA in coordination with EPA) providing the technical support would determine the appropriate prioritization order based on the water system responses and the totality of the circumstances, such as:

- The risk to water system operations and potential adverse impacts on the service area, downstream critical infrastructure, and defense/national security assets,
- The capabilities of a water system to remediate the vulnerability without Federal support, and
- The risk reduction benefits that technical cybersecurity support from CISA or EPA would achieve.

Table 1 below lists the required statutory criteria for the Prioritization Framework, the associated questions that a water system would answer when requesting cybersecurity technical support under a surge scenario where use of the Framework was needed, and considerations that EPA or CISA could apply when determining a prioritization order.

Note that the order in which the criteria are listed in Table 1 does not imply preferential weighting for prioritization rank. Rather, weighting would be based on the threat circumstances and the needs of water systems for technical cybersecurity support.

Table 1: PRIORITIZATION FRAMEWORK CRITERIA, QUESTIONS, AND AGENCY CONSIDERATIONS

| **Statutory criteria from Sec. 1420A(b)(1)** | **Questions for water systems requesting technical cybersecurity support** | **Considerations by EPA or CISA in prioritizing water systems for assistance** |
|---|---|---|
| (A)…identify public water systems (including sources of water for those public water systems) that, if degraded or rendered inoperable due to an incident, would lead to significant impacts on the health and safety of the public | How many people does the water system or source serve (including consecutive systems and those technologically integrated)?<br><br>Does the service area have resources (e.g., alternative sources of supply) that could mitigate the impact of degraded water service?<br><br>Note: Downstream critical infrastructure, such as health care, is addressed in a separate criterion. | Priority would increase with greater population served (i.e., adverse impacts from water service degradation would grow with higher population served).<br><br>Priority would decrease for water systems where the service area has greater resources to mitigate impacts of degraded water service. |
| (B)(i) whether cybersecurity vulnerabilities for a public water system have beenidentified under Section 1433 | Did the water system conduct a risk and resilience assessment under America's Water Infrastructure Act that included cybersecurity (required for community water systems serving over 3,300 people)?<br><br>Did the water system conduct an alternative cybersecurity vulnerability assessment (e.g., CISA Cyber Hygiene services, EPA Technical Assistance Provider program, NIST Cybersecurity Framework, or private sector assessment)? | Whether a water system had conducted a cybersecurity vulnerability assessment would not be a factor in decisions by EPA or CISA to provide critical technical cybersecurity support.<br><br>If a water system reported that it had identified a vulnerability under an assessment but had not yet addressed the vulnerability, EPA or CISA would consider whether that vulnerability would increase the need for assistance under the threat circumstance. Regardless of priority, EPA and CISA would encourage the water system to correct the deficiency and would assist the water system where needed.<br><br>Furthermore, if a water system requested technical cybersecurity support and had not assessed cybersecurity vulnerabilities, EPA and CISA would, in addition to providing the requested support, encourage the water system to do so and would assist the water system where needed. |

| Statutory criteria from Sec. 1420A(b)(1) | Questions for water systems requesting technical cybersecurity support | Considerations by EPA or CISA in prioritizing water systems for assistance |
|---|---|---|
| (B)(ii) the capacity of a publicwater system to remediate a cybersecurity vulnerability without additional Federal support | What near- and long-term internal technical capabilities and financial resources does the water system have to correct cybersecurity vulnerabilities?<br>How urgent is the water system's need for technical cybersecurity assistance?<br>Are other external sources of technical cybersecurity support (e.g., other government or private sector assistance providers) available to the water system? | A water system with an urgent need for technical cybersecurity support (e.g., a known vulnerability that poses a significant risk to the water system's operations) and that lacks either internal or external technical or financial resources to correct the vulnerability in a sufficient time frame would be prioritized for assistance. |
| (B)(iii) whether a public water system serves a defense installation or critical national security asset | Does the water system serve a defense installation or national security asset (e.g., defense production facility, communications provider, etc.)? | Serving a defense installation or national security asset would be a significant prioritization factor for technical cybersecurity support. |
| (B)(iv) whether a public water system, if degraded or rendered inoperable due to an incident, would cause a cascading failure of other critical infrastructure | What critical infrastructure facilities does the water system serve (across all 16 critical infrastructure sectors)? | Water systems that serve a greater number of critical infrastructure facilities would be prioritized for technical cybersecurity support.<br>Further, water systems that serve critical infrastructure facilities where a degradation in water service would cause especially severe consequences (e.g., health care facilities) would be prioritized for support |