ASSOCIATION OF METROPOLITAN WATER AGENCIES

LEADERS IN WATER

1620 I Street, NW, Suite 500
Washington, DC 20006

P 202.331.2820
amwa.net

November 14, 2022

Mrs. Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency (CISA)
Department of Homeland Security
Washington, DC 20528

Via electronic submission

Re: Docket ID: CISA–2022–0010; Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

Dear Director Easterly,

The Association of Metropolitan Water Agencies (AMWA) appreciates the opportunity to provide these comments in response to CISA's Request for Information (RFI) to inform the agency's development of new critical infrastructure cyber incident reporting rules enacted by Congress through the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022. As an organization representing the largest publicly owned drinking water systems in the United States, whose members generally serve more than 100,000 people, we anticipate that many of our member utilities will be considered "covered entities" under CIRCIA. Our comments in response to this request for information are therefore intended to highlight several high-priority issues for these water systems with the intent of making the eventual incident reporting requirements as workable and beneficial as possible.

Our comments will not touch on every component of the RFI, but we have identified the following terms and requirements as especially consequential for community water systems that may be affected by CIRCIA's reporting requirements.

Covered Entity

Section 2240 of the Homeland Security Act, as amended by CIRCIA, defines a "covered entity" as "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b)."

Presidential Policy Directive 21 (PPD21) identifies 16 critical infrastructure sectors, including "Water and Wastewater Systems."

Section 2242(c) of the Homeland Security Act, as amended by CIRCIA, specifies that the final rule promulgated pursuant to section 2242(b) shall include "a clear description of the types of entities that constitute covered entities," based on:

- "The consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;"
- "The likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country;" and
- "The extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure."

It is apparent that based on PPD21, at least some portion of the nation's roughly 50,000 community water systems will be considered "covered entities" under CIRCIA. However, it is clear that Congress did not intend for every community water system captured by PPD21 to be subject to CIRCIA, because in that case it would not be necessary for Section 2242(b) to define the "types of entities" in a critical infrastructure sector that will be subject to CIRCIA. CISA must therefore determine when a cyber-attack against a community water system would disrupt national or economic security or public health and safety, how likely such an attack would be, and the extent to which the incident could disrupt the reliable operation of critical infrastructure.

Answering these questions is difficult. As was demonstrated by the 2021 intrusion into the drinking water system serving Oldsmar, Florida (population approximately 15,000), even community water systems serving relatively small communities are not immune from cyber-attacks. However, while the Oldsmar incident had the potential to compromise "public health and safety" of those served by the water system, it is unlikely that there would have been broader direct national implications from the event had the attack actually affected the community's water quality.

On the other hand, a successful attack against a community water system serving a major metropolitan area would likely have broader national security and economic security consequences, and could also affect a wide range of assets in other critical infrastructure sectors.

Given these factors, AMWA believes that CISA's description of the types of community water systems that should be considered "covered entities" under CIRCIA should include:

- A service population threshold, below which a community water system shall generally not be considered a covered entity;
- A service population threshold, above which a community water system shall generally be considered a covered entity; and
- Guidelines for designating community water systems whose service populations fall between the two thresholds as covered entities if they provide water service to other specified critical infrastructure assets whose reliable operations would be interrupted in the event of a major cyber-attack against the community water system.

This approach is intended to be based in simplicity and predictability by generally excluding or including certain community water systems based on their service populations and therefore the likely breadth of the ramifications of a successful cyber-attack. But it also recognizes that other community water systems provide service to nationally-important critical infrastructure assets that could be affected as a result of an attack, and therefore should qualify as "covered entities" for the purposes of cyber incident reporting.

However, we expect that the owners or operators of certain critical infrastructure entities that do not fall under the definition of "covered entities" may nevertheless wish to report cyber incidents to CISA. This type of voluntary reporting should be encouraged, therefore the information reporting system established by CISA should include a simple mechanism to invite the voluntary submission of reports.

Covered Cyber Incident

Section 2240 of the Homeland Security Act, as amended by CIRCIA, defines a "covered cyber incident" as "a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2242(b)."

Section 2242(c) of the Homeland Security Act, as amended by CIRCIA, specifies that the final rule promulgated pursuant to section 2242(b) shall include "a clear description of the types of substantial cyber incidents that constitute covered cyber incidents," which at a minimum shall:

- Lead "to the substantial loss of confidentiality, integrity, or availability" of an information system or network, or carry a serious impact on the safety and resiliency of operational systems and processes;
- Disrupt business or industrial operations; or
- Involve unauthorized "access or disruption of business or industrial operations due to a loss of service" due to the compromise of a cloud service or third-party data hosting provider.

CISA is also directed to consider "the sophistication or novelty" of the cyber incident, the number of individuals affected, and "potential impacts on industrial control systems."

Based on these factors, AMWA believes that a "covered cyber incident" which triggers reporting requirements for covered community water systems under CIRCIA should constitute an unauthorized or malicious act that materially interrupts, or threatens to interrupt, the operation of an industrial control system, necessitating corrective actions by the community water system to maintain operations. This standard for this type of attack is consistent with the requirements of CIRCIA because it remains relatively novel and, to be successful, would require a level of sophistication beyond what may be encountered in a "routine" attack.

Events that should not be considered a "covered cyber incident" under CIRCIA are these "routine" incidents targeting a system's information technology. Such "routine" incidents, like phishing attempts, may be viewed as those that may be encountered by any internet user, and do not necessarily and uniquely target community water system operations or critical infrastructure. Casting too wide a definition of a "covered cyber incident" would burden covered entities with excessive reporting requirements, and overwhelm CISA with data that could obscure truly significant cyber-attacks that require the most attention and response.

Substantial Cyber Incident

Section 2240 of the Homeland Security Act, as amended by CIRCIA, defines a "covered cyber incident" as "a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2242(b)." However, while the revised Act proceeds to define a "significant cyber incident" as "a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States," CIRCIA does not provide a definition for a "substantial cyber incident." Therefore, it is unclear whether Congress intended for the terms "significant" and "substantial" cyber incidents to be used interchangeably, or if lawmakers were deliberate in making a distinction between the two.

Since the Request for Information seeks input on the meaning of "substantial cyber incident," AMWA believes that CISA intends to make a distinction between the two terms. In that case, we understand that, based on the Section 2240 definition of "covered cyber incident," all covered cyber incidents must also be substantial cyber incident, but not all substantial cyber incidents will necessarily be covered cyber incidents. Therefore a "substantial cyber incident" does not necessarily have to:

- Lead "to the substantial loss of confidentiality, integrity, or availability" of an information system or network, or carry a serious impact on the safety and resiliency of operational systems and processes;
- Disrupt business or industrial operations; or
- Involve unauthorized "access or disruption of business or industrial operations due to a loss of service" due to the compromise of a cloud service or third-party data hosting provider.

A "substantial cyber incident" should still represent more than a "routine" event like a phishing attempt against a covered entity's IT network. CISA may wish to define it as the intentional, targeted, and unauthorized accessing of a covered entity's operational systems, which has the potential to result in an extended outage of the core services provided by the entity.

Cyber Incident Reporting Following a Reasonable Belief of an Attack

Section 2242(a)(1)(A) of the Homeland Security Act, as amended by CIRCIA, requires that a covered entity "that experiences a covered cyber incident shall report the covered cyber incident to [CISA] not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred."

The RFI seeks input on what constitutes "reasonable belief" that a covered cyber incident has occurred, thereby triggering the 72-hour reporting requirement.

Before coming to the "reasonable belief" that a covered cyber incident has occurred, a covered entity must first make a number of determinations. First, it must observe unexpected or unusual behavior within its computer network. Then, it must investigate the cause of this unexpected or unusual behavior, and determine whether it is likely to be the result of unauthorized access to the system. If the behavior is determined to be the result of unauthorized access, the covered entity must then determine whether this unauthorized access represents a "substantial cyber incident," based on CISA's ultimate definition of that term. Then, the covered entity must determine whether the unauthorized access represents a "covered cyber incident," based on the parameters set by Congress in Section 2242(c) and CISA's ultimate definition of the term. Only at that point, if the covered entity comes to conclude that the unauthorized access may represent a "covered cyber incident" will it have obtained a "reasonable belief" that such an incident has occurred. Only from that point should the 72-hour reporting requirement begin to be measured.

It is important to remember that a covered entity will be going through this process against the backdrop of an unfolding cyber incident, during which the immediate priority will be securing the system and limiting the potential damage – not comparing the features of the cyber incident to the definitions of terms in CIRCIA. AMWA therefore believes that covered entities should be afforded significant flexibility in this regard, and that a covered entity should not be considered to have a "reasonable belief" that a covered cyber incident has occurred until it has had ample

opportunity to analyze the event, consult with cybersecurity experts, and rule out benign causes of the event. As a result, the 72-hour reporting requirement should not begin to be measured until all these activities have been completed.

This may introduce additional time between the cyber-attack and when the report reaches CISA, but it also means that these reports are more likely to represent actual covered cyber incidents deserving of CISA's attention. Requiring the reports to be submitted too early, before an entity can be sure of what happened, would risk overwhelming CISA with "false alarm" or speculative reports, and represent a waste of resources among covered entities.

Contents of Required Reports

Section 2242(c)(4) of the Homeland Security Act, as amended by CIRCIA, specifies certain information that shall be included in an incident report required to be submitted to CISA within 72 hours following the reasonable belief of a covered cyber incident, "to the extent applicable and available." Among the information the statute mandates to be contained within the report includes:

- The affected information systems, networks, or devices;
- A description of the unauthorized access;
- The estimated date range of the incident;
- The impact to the operations of the covered entity;
- The vulnerabilities exploited and the security defenses that were in place;
- The tactics, techniques, and procedures used to perpetrate the incident;
- Any identifying or contact information related to each actor reasonably believed to be responsible for the incident;
- Identification of the category or categories of information that were thought to have been, accessed or acquired by an unauthorized person; and
- Contact information for the covered entity.

The RFI seeks input on the specific information that should be required to be included in the reports, taking into consideration these requirements of Section 2242(c)(4).

AMWA strongly urges CISA to be mindful that much of this information will not be readily available to the victim of a cyber-attack, and certainly not within the first 72 hours of the realization that an attack has taken place. For example, while it would be prudent and reasonable for a covered entity to promptly report to CISA on the estimated timing of the incident, the types of devices believed to be affected, the known impacts on system operations, and contact information of the covered entity, other information specified in Section 2242(c)(4) may be much harder for a covered entity to obtain at all – let alone within 72 hours.

Information that could be much more difficult to accurately report within 72 hours includes the specific system vulnerabilities exploited, the tactics and techniques used by the perpetrator(s), and identifying or contact information of the attacker(s). Fortunately, Section 2242(c)(4) recognizes this by specifying that the 72-hour report must only include such information "to the extent applicable and available." CISA therefore should only require that this 72-hour report only include such information that the covered entity has readily available with a reasonable degree of accuracy. This will ensure that CISA has essential, timely information about recently unfolding incidents, which should help the agency identify patterns and notify other critical infrastructure entities about potential threats.

Beyond the initial mandated 72-hour report, CISA may wish to encourage covered entities to submit additional detailed information about covered incidents at a later date, when more is known about the scope, impacts, and perpetrators of the incident. This will allow victims of cyber-attacks to focus on their response and recovery in the immediate aftermath of the incident, while also increasing the accuracy and usefulness of information about the incident that is eventually provided to CISA.

Ransom Payment Reporting

Section 2240 of the Homeland Security Act, as amended by CIRCIA, defines a "ransom payment" as "the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack."

Section 2242(a)(2)(A) of the Homeland Security Act, as amended by CIRCIA, requires "a covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours after the ransom payment has been made."

The RFI seeks input as to when the 24-hour-post-ransom-payment-reporting timeframe should begin. It is AMWA's opinion that this clock should not begin ticking until the moment that a covered entity has actually taken an action to transmit a ransom payment to the attacker, in whatever form the ransom is provided (such as legal tender, digital currencies, gift cards, or any other store of value demanded by the cyber attacker). If a covered entity makes a ransom payment during non-business hours, the 24-hour reporting clock should begin ticking at the onset of the next business day.

AMWA further believes that CISA must establish and widely publicize a secure platform through which covered entities can easily transmit their required reports on covered incidents and ransom payments with minimal paperwork. Otherwise, important resources may be diverted to fulfilling reporting requirements amid the covered entity's response to the attack.

Third-Party Incident Reporting

Section 2242(d)(1) of the Homeland Security Act, as amended by CIRCIA, allows a covered entity to "use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit" a required incident report.

The RFI seeks examples to what type of entities may constitute third parties that may submit a covered cyber incident report or ransom payment report on behalf of a covered entity.

AMWA believes that CISA should clearly and unambiguously recognize the various Information Sharing and Analysis Centers, or ISACs, as entities that may be utilized by a covered entity to submit required incident and ransom reports to CISA. In the case of the water sector, WaterISAC is the sector's dedicated information sharing resource that provides actionable threat info and recommended response actions to water systems, in relation to a wide range of potential threats. As such, WaterISAC maintains positive working relationships with DHS, EPA, and other regulators and stakeholders, while also regularly interfacing with community water systems.

WaterISAC also collects reports of unfolding cyber incidents from community water systems, so that could position it to pass information it receives from a covered entity on to CISA – thereby saving a step for the covered entity and giving it more time to focus on responding to the cyber event. Similarly, the Multi State Information Sharing and Analysis Center (MS-ISAC) provides cyber threat resources and incident reporting services to state, local, and Tribal governments across the country. Especially given that many covered entities may have limited past direct interaction with CISA, it would be beneficial to utilize this existing network of ISACs for the purpose of delivering required cyber incident reports to the agency.

Thank you for providing the opportunity to offer comments to the RFI. AMWA and its members look forward to continuing to provide feedback and perspectives as CISA continues the process of developing CIRCIA recommendations. If you have any questions, please feel free to contact Brian Redder, AMWA's Manager of Regulatory and Scientific Affairs, at redder@amwa.net.

Sincerely,

Thomas Dobbins
Chief Executive Officer

cc: Todd Klessman, CISA
Jennifer McLain, USEPA
Radhika Fox, USEPA