ASSOCIATION OF METROPOLITAN WATER AGENCIES

The Cyber Incident Reporting for Critical Infrastructure Act of 2022

Approved by the House of Representatives on March 9, 2022 and the Senate on March 10 as Division Y of H.R. 2471, the Consolidated Appropriations Act of 2022.

Brief summary:
This legislation amends the Homeland Security Act of 2002 (6 U.S.C. 651) to require covered critical infrastructure owners and operators to report defined cyber incidents to DHS' Cybersecurity Information and Security Agency (CISA) within 72 hours of having a reasonable belief that an incident has occurred. Covered entities would also have to report to CISA within 24 of making a ransom payment related to a cyber incident, after considering alternatives to making the ransom payment. CISA will conduct rulemaking to develop the details of the program, including precise definitions of "covered entities" subject to the reporting requirements.

Applicability to water systems:
While the legislation makes no reference to drinking water or wastewater utilities, it is highly likely that at least some systems will meet the definition of "covered entities" subject to the law, when CISA completes its rulemaking. However, the water sector and other stakeholders will have an opportunity to engage with CISA and submit comments on the proposed rule as it is developed and finalized. The legislation could also present opportunities for WaterISAC to serve as a conduit for cyber threat information between CISA and water systems, and to aid water systems in submitting required incident and ransom reports to the agency.

Specific additions to the Homeland Security Act:

1. **A new section 2241 will direct the National Cybersecurity and Communications Integration Center (NCCIC) to take several actions, including:**

    a. Receive, aggregate, analyze, and secure cyber incident reports submitted by covered entities, for the purpose of assessing the effectiveness of security controls and identifying tactics used by adversaries to overcome those controls;

    b. Coordinate and share information with federal departments and agencies to identify and track ransom payments;

    c. Leverage information collected about cyber incidents to:

        i. Enhance the quality and effectiveness of information sharing efforts with appropriate entities, including state, local, tribal, and territorial

governments, critical infrastructure owners and operators, sector coordinating councils, and Information Sharing and Analysis Organizations;

ii. Provide these same appropriate entities with timely, actionable, and anonymized reports of cyber incident trends;

d. Facilitate the timely, voluntary sharing of information related to covered cyber incidents and ransom payments, between relevant critical infrastructure owners and operators;

e. Review the details of significant cyber incidents to identify and disseminate ways to prevent or mitigate similar incidents in the future; and

f. Publish quarterly unclassified, public reports that describe aggregated, anonymized findings and recommendations based on covered cyber incident reports.

2. A new section 2242 will impose new cyber incident reporting mandates that:

a. Require covered critical infrastructure entities to report covered cyber incidents to CISA within 72 hours after having a reasonable belief that the covered cyber incident has occurred;

b. Require covered critical infrastructure entities to report ransom payments made as a result of a ransomware attack to CISA within 24 hours of making the payment;

c. Require covered infrastructure entities to update or supplement previously submitted incident reports if substantial new or different information about the incident becomes available;

d. Require covered critical infrastructure entities to preserve data relevant to the cyber incident or ransom payment;

e. Direct CISA to publish a notice of proposed rulemaking to implement the incident reporting requirements, not later than 24 months after enactment of the legislation;

f. Direct CISA to finalize the rulemaking not later than 18 months after publishing the notice of proposed rulemaking;

g. Specify that the final rule shall include:

i. A definition of covered entities, based on:

1. The consequences that a cyber attack against the entity could cause to national security, economic security, or public health and safety;

2. The likelihood that such entity may be targeted by a malicious cyber actor; and

3. The extent to which damage, disruption, or unauthorized access to such entity will likely enable the disruption of the reliable operation of critical infrastructure;

ii. A definition of covered cyber incidents, which must include, among other factors, the substantial loss of confidentiality, integrity, of an information system or network, or serious impact on the safety and resiliency of operational systems and processes;

iii. A description of the specific required contents of incident reports;

iv. Procedures for covered entities to submit required incident and ransom reports;

h. Allow covered entities to submit incident or ransom payment reports to CISA via a third party, such as an Information Sharing and Analysis Organization; and

i. Require CISA to conduct an outreach and education campaign to inform likely covered entities and other appropriate entities about the new reporting requirements.

3. **A new section 2243 will allow entities to voluntarily report cyber incidents to CISA**

4. **A new section 2244 will allow CISA to enforce the incident reporting requirements, including through:**

    a. Issuing a subpoena to a covered entity if it has not reported a suspected incident or ransom payment after 72 or 24 hours, respectively.

5. **A new section 2245 will outline the use and protection of cyber incident information shared with the federal government, including:**

    a. Prohibiting the use of cyber incident or ransom reports to support regulatory or enforcement actions;

    b. Exempting cyber incident and ransom reports submitted to CISA from disclosure under the federal Freedom of Information Act or similar state or local laws;

    c. Enacting liability protections for entities that submit cyber incident or ransom reports in accordance with this act.