AMWA requests workable cyber incident reporting rules

November 21, 2022 at 12:26 PM

AMWA last week submitted comments (https://www.amwa.net/testimonycomments/comments-cyber-incident-reporting-request-information) to the Cybersecurity and Infrastructure Security Agency (CISA) that offered guideposts for how the agency can make upcoming critical infrastructure cyber incident reporting rules "as workable and beneficial as possible." Under legislation approved (https://www.amwa.net/article/congress-approves-cyber-incident-reporting-legislation) by Congress earlier this year, CISA is required to propose cyber incident reporting rules for covered critical infrastructure entities by early 2024.

In September, CISA released (https://www.amwa.net/article/cisa-seeks-perspectives-cyber-incident-reporting-rules-launches-listening-sessions) a Request for Information (RFI) that sought stakeholder perspectives to inform the development of the regulatory proposal. AMWA's comments in response to the RFI – which were informed by input from the association's Regulatory and Security committees – recommended approaches to defining key terms in the statute like "covered entity" and "covered cyber incident," and suggested what information should be included in incident reports that must be submitted to CISA within 72 hours of a reasonable belief that an attack has taken place. On this point, AMWA noted that much information about a cyber incident and its perpetrator "will not be readily available to the victim … within the first 72 hours of the realization that an attack has taken place." Therefore, the association recommended that the initial report only be required to include information readily available "with a reasonable degree of accuracy."

AMWA further recommended that sector information sharing and analysis centers like WaterISAC be "clearly and unambiguously" recognized in the regulation as being allowed to submit an incident report on behalf of a covered entity. AMWA noted that WaterISAC can be a liaison to provide these reports because it "maintains positive working relationships with DHS, EPA, and other regulators and stakeholders, while also regularly interfacing with community water systems."

CISA's regulation will ultimately determine which critical infrastructure entities are subject to the reporting requirement, but AMWA anticipates that many large drinking water systems will likely be covered. The association's comments did not attempt to draw the line at where coverage should begin but did say that CISA should define "a service population threshold, above which a community water system shall generally be considered a covered entity," thereby giving water systems some degree of certainty about their status.

After CISA proposes its cyber incident reporting rules in early 2024, the agency will be

required to finalize them by late 2025.

Back to *November 21, 2022* (https://www.amwa.net/monday-morning-briefing/november-21-2022)
