Senate quickly approves new cyber incident reporting rules

March 7, 2022 at 5:00 AM

Against the backdrop of Russia's invasion of Ukraine and escalating concerns about potential cyberattacks, the Senate last week unanimously approved (https://www.hsgac.senate.gov/media/majority-media/senate-passes-peters-and-portman-landmark-legislative-package-to-strengthen-public-and-private-sector-cybersecurity-) a package of cybersecurity legislation that includes provisions that would require certain critical infrastructure owners and operators to promptly report cyber intrusions to DHS. While water and wastewater systems are not specifically referenced in the bill, the new reporting rules would likely apply to at least some large water utilities.

The Strengthening American Cybersecurity Act (S. 3600 (https://www.hsgac.senate.gov/imo/media/doc/Peters_Strengthening%20American%20Cybersecurity%20Act%20Text.pdf)) is composed of a package of several different cyber bills previously passed by the Senate Homeland Security and Governmental Affairs Committee, including an incident reporting bill that the committee approved (https://www.amwa.net/article/cyber-incident-reporting-bill-gets-senate-panel-okay) last October.

The incident reporting provisions of the new legislation appear to mirror those of the old, such as by requiring covered critical infrastructure owners and operators to report to the Cybersecurity Information and Security Agency (CISA) within 72 hours of a reasonable belief that they have experienced a cyberattack. Covered entities also would have to report to CISA within 24 hours of making a ransom payment and consider alternative options before paying. Other parts of the bill would limit how information contained within reports could be used and would allow CISA to subpoena information about cyberattacks that are not reported pursuant to the legislation.

While S. 3600 does not call out water systems as subject to the reporting requirements, the bill would charge CISA with undertaking a rulemaking to define which critical infrastructure entities are covered by the reporting rules. It is therefore likely that at least some major drinking water systems would be covered, particularly if there is a belief that a successful cyberattack against them could lead to significant public health or economic consequences.

The legislation also recognizes a role for Information Sharing and Analysis Organizations (ISAOs), like WaterISAC (https://www.waterisac.org/), to play in the incident reporting and cyber preparedness landscape. The bill would direct CISA to provide certain entities, including sector ISAOs, with "timely, actionable, and anonymized reports" about cyber incidents and trends, while directing CISA to enhance the quality and effectiveness of its information sharing and coordination efforts with these entities. Critical infrastructure entities required to report cyber incidents to CISA would also be permitted to do so via their sector's ISAO.

S. 3600 quickly and unanimously passed the Senate last week under a procedure known as "unanimous consent," which allows legislation to advance with minimal debate, provided that no senator objects. Sponsors of the combined cybersecurity measure had introduced (https://www.amwa.net/article/cyber-incident-reporting-legislation-resurfaces-senate) the bill last month, at which time there were no indications it was on a fast track to passage. But the war in Ukraine elevated the issue, so the measure will now move on to the House of Representatives for consideration.

Back to *March 7, 2022* (https://www.amwa.net/monday-morning-briefing/march-7-2022)