# The Cyber Clock is Ticking: Biden Administration & Congress Advance Incident Reporting

**09.23.2021 | By Hon. Chris Carney**

As we reported on September 9th, meaningful and robust federal cybersecurity legislation is nearly across the finish line. Since then, further developments indicate that reporting mandates are imminent. On September 21st, the United States Department of the Treasury's Office of Foreign Asset Control (OFAC) released guidance that all U.S. companies not reporting ransomware attacks would be subject to enforcement action and possible fines. The Biden administration was on Capitol Hill on September 22nd to press the issue forward.

U.S. Department of Homeland Security (Homeland) Secretary Alejandro Mayorkas intimated support for requirements that all critical infrastructure providers report cyberattacks in a timely fashion. Mayorkas suggested that various agencies of the U.S. government have methods to restore compromised data without paying ransoms; but speed in reporting a breach is critical. During testimony to Congress on the same day, Jen Easterly, Director of the Homeland's Cybersecurity and Infrastructure Security Agency (CISA), called for a 24-hour reporting window for ransomware attacks. Easterly said the faster an attack is reported, the more likely it is additional attacks will be prevented. Leading up to this, Easterly and Chris Inglis, the National Cyber Director, have both supported levying fines on companies that do not provide timely reporting, including critical infrastructure providers and government contractors.

This comes on the heels of bipartisan consensus building in Congress over the summer for:

- Authorizing federal government funding for industries that have historically been lacking in cybersecurity preparedness and response;
- Vesting legal authorities in the federal government to provide preparedness and response capabilities, including funding to impacted industries; and

- Meaningful cybersecurity measures, including a 72-hour reporting time window for cybersecurity incidents, and more.

Several pieces of legislation pending in Congress have cybersecurity provisions that would impact the electric grid, water facilities, primary K-12 schools and others the federal government may decide constitute "critical infrastructure."

The pending *National Defense Authorization Act of 2021* (NDAA), H.R. 4350 (117th Cong.) would create a Cyber Incident Review Office (CIRO) in CISA. This is sponsored by a bipartisan group of legislators who have jurisdiction over cybersecurity. They are Homeland Security Chairman Bennie G. Thompson (D-MS), Cybersecurity Infrastructure Subcommittee Chair Yvette Clarke (D-NY), Homeland Security Committee Ranking Member John Katko (R-NY) and Cybersecurity Infrastructure Subcommittee Ranking Member Andrew Garbarino (R-NY). Reports will be required and information will be collected by the federal government from entities it determines own or operate "critical infrastructure."

If enacted via the NDAA, the CIRO would receive, aggregate and analyze reports related to covered cybersecurity incidents and would have broad powers to acquire information and reporting details of cyber incidents. CIRO, working through the Secretary of Homeland Security, will have the ability to issue an interim rule about nine months after enactment. Then, about a year and nine months later, they would issue a final regulation. These regulations will be relevant to the CIRO reporting and will determine which entities are subject to the CIRO reporting.

If enacted, the new law would require the Director of CISA to issue within 270 days after enactment an interim final rule implementing this new law (effective once published in the Federal Register). The interim final rule is to include (1) a description of the types of critical infrastructure entities that fall the new law; (2) the types of cybersecurity incidents that are determined to fall within the requirements of the law; and (3) the mandatory reporting requirements and processes for reporting that need to be followed by these covered entities when they experience a "significant cyber incident." Failure to meet mandatory reporting requirements may result in an investigatory subpoena and potential referral to the Attorney General for civil or criminal prosecution of anyone who fails to meet the new requirements.

Before publishing the interim final rule, the Director of CISA is to consult with Sector Risk Management Agencies and the heads of other Federal departments and agencies, followed by a 90-day comment period with appropriate stakeholders, including sector-coordinating councils. While the interim final rule is to go into effect immediately upon publication, it may be subject to change and revision after a public notice and comment period. This will be an extremely limited and crucial time to affect the interim regulation.

The increase of cyberattacks, including ransomware, have severely impacted the United States economy. The Biden Administration is taking a "whole of government" approach to discourage ransomware and cyber incidents. In the last few days, the Biden Administration has moved quickly to attempt to alter the cybersecurity threat landscape.

Unlike other countries in the world where the government controls access to the internet and critical infrastructure, the United States has relied heavily on the private sector to increase cybersecurity capabilities. This is because, in the United States, 85% of critical infrastructure is privately owned. However, the private sector cannot cover the remaining 15% of critical infrastructure that is not in private hands. Thus, there is a gap in addressing cyber needs of extremely important but vulnerable utilities, including water

systems.

Consider the potential impact of a cybersecurity or ransomware attack on a water system, similar to the February 2021 cyberattack on the water supply of the City of Oldsmar, Florida in the Tampa Bay. The vulnerability of and potential impact on local and municipal water entities and the customers they serve becomes clear. The Oldsmar hacking, an attempt to poison the water supply, was detected in time to prevent contamination of the water supply serving the area around the Super Bowl. But it could have been catastrophic and could have led to a mass casualty event. Federal legislators and cybersecurity regulators are concerned enough that bipartisan Congressional support has emerged for cybersecurity vulnerability assessments for water entities and has been included in the Bipartisan Infrastructure Framework legislation that has passed the U.S. Senate and is now under consideration in the U.S. House.

Significant cybersecurity legislation is coming, and the clock is ticking for entities that are regulated. Those deemed to own or operate “critical infrastructure” need to prepare for the creation and implementation of these new rules.