Public and Private Stakeholders: Get the Federal 'Cyber Carrots' Now Because the Stick is Coming!

09.09.2021 | By Hon. Chris Carney, Frederick T. Dombo III, D. Michael Stroud Jr.

In the wake of several recent high-profile cyber and ransomware attacks on critical infrastructure, Committees in both the House and Senate are drafting at least three separate pieces of legislation that would require victims of attacks to report them to the Cyber and Infrastructure Security Agency (CISA) and National Institute of Standards and Industry (NIST) within a specified time frame or potentially face punitive actions.

A **24 hour reporting obligation** was included in the first piece of legislation introduced in July by Senate Intelligence Committee Chair Mark Warner (D-VA) and Vice Chair Marco Rubio (R-FL) as S. 2407. This bill would require critical infrastructure operators to report successful or attempted attacks to CISA within 24 hours or face fines up to 0.5% of their previous year's gross revenue for every day it fails to report the attack. Senate Homeland Security and Governmental Affairs Chair Gary Peters (D-Mich.) said earlier that he's working on cyber incident reporting legislation with Ranking Member Rob Portman (R-OH), but the committee hasn't announced legislation timing, nor has a bill number been assigned.

Draft legislation from the House Homeland Security Committee, referred to as the *Cyber Incident Reporting for Critical Infrastructure Act of 2021*, is also in its final development. The bipartisan draft bill would create a new **Cyber Incident Review Office**, define what a "significant" cyberattack entails and determine how a covered entity would report an attack, as well as how CISA will enforce reporting noncompliance. This framework would be created by a currently unnumbered House bill authored by Cybersecurity, Infrastructure Protection, and Innovation Subcommittee Chair Yvette Clark (D-NY) and supported by Homeland Security Committee Chair Bennie Thompson (D-MS) and Ranking Member John Katko (R-NY). The bill would also call for CISA to issue an interim "final rule" within nine months to require critical

infrastructure operators, such as energy companies, pipeline operators, water companies, hospitals, etc. to report cyber incidents within 72 hours after they occur. The new office would be housed within CISA to aggregate and analyze cyber reports from covered companies. While the bill does not set penalties for failure to report in a timely manner, it does direct CISA to establish exactly which critical infrastructure entities would be required to report cyberattacks. Based on testimony from a broad spectrum of industry stakeholders, the bill and its approaches enjoy industry support.

Lastly, while the bills mentioned above are not quite yet mature enough for imminent legislative action, the Congressional action to include the "Cyber Response and Recovery Act of 2021" (CRRA), introduced by Senators Peters and Portman, in the Bipartisan Infrastructure Framework (BIF) (i.e., the bipartisan infrastructure legislation) is the strongest indication of bipartisan agreement on core components of cybersecurity policy. CRRA, along with other legislation, including the *State and Local Cybersecurity Improvement Act,* embody a few of the more prominent recommendations. CRRA establishes:

- The United States Department of Homeland Security as the lead for private industry, state, local and tribal government cyber incident reporting and response, with a limited consultation role with the National Cyber Director;
- A $20 million dollar cyber response fund; and
- The ability for private and public entities to access the cyber response fund, among other responsibilities.

The steps taken to include the CRRA and the *State and Local Cybersecurity Improvement Act* indicate that Congress feels pressure to create a robust cybersecurity regulatory regime for our nation's critical infrastructure systems. Expect punitive cybersecurity legislation to be forthcoming. Obviously, critical infrastructure providers favor the House bill that allows a 72-hr reporting window for cyberattacks and that does not specify any penalties for noncompliance. However, should the current House and Senate conference over their differing bills, such as the BIF or any imminent funding legislation, the regulated community should expect some sort of financial consequences against critical infrastructure providers who do not report attacks on the regulators' schedule.

In the meantime, cities that have not already done so should look into the resources available from the federal government to assess and address their vulnerabilities. Besides CISA's ongoing work of conducting free cybersecurity assessments of city government systems, state, local and tribal entities will want to learn more about the State and Local cybersecurity provisions in the BIF. Specifically, the Department of Homeland Security has grants available to help cities address any deficiencies found. Additionally, the *State and Local Cybersecurity Improvement Act*, which is included in the BIF, is also designed to help state, local and tribal entities identify and address cybersecurity issues and vulnerabilities. A provision in the BIF also allows for grant funding for governmental entities to help identify cyber vulnerabilities.

There is currently a window of opportunity to shape regulatory parameters in the final legislation and as the agencies begin the implementation of legislation. However, the window for shaping this is likely closing in the next several months.