BRACEWELL

INSIGHTS

The US Government Has a New Stopwatch for Cyber Incident Reporting: What You Need to Know Now

March 16, 2022

*By: **Seth D. DuCharme** and **Anissa L. Adas***

Amid the escalating conflict in Ukraine and concerns of Russian cyber threats to the United States, President Joe Biden recently signed a $1.5 trillion government spending ***deal*** with serious cybersecurity reporting obligations for critical infrastructure operators intended to shore up protection of American infrastructure. The Strengthening American Cybersecurity Act —attached to the spending package that funds the federal government until September —requires "critical infrastructure operators" to report cyber incidents to the DHS Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours of a cyber-attack, and within 24 hours of a ransomware payment. In light of the new requirements, companies should ensure that their critical incident response plan can function at the required tempo.

Companies considered "critical infrastructure" and subject to the reporting requirements include those in the energy, food and agriculture, information technology, transportation systems, healthcare and public health, commercial facilities, and communications industries, among others.[1] Companies who abide by the new reporting measures, can expect limited liability, and trade secret protection in exchange for their compliance. The bill also grants CISA the power to subpoena entities that don't report a cyber incident or ransomware payment and the ability to make referrals to the Department of Justice for enforcement actions. Noncompliant companies could also face debarment and other financial penalties.

House and Senate members have praised the bill as timely, particularly as cybersecurity concerns continue to rise as a result of U.S. sanctions against Russia for its invasion of Ukraine. "The Cyber Incident Reporting for Critical Infrastructure Act, included within the Consolidated Appropriations Act, 2022, is one of the most significant pieces of cybersecurity legislation in the past decade," said representatives for the Committee on Homeland Security in a press release issued just the day before the bill's passage.

An added goal of the reporting requirements is to strengthen relationships between the public and private sectors. CISA Director Jen Easterly ***called*** the bill a "game-changer," also saying that "CISA will use these reports from our private sector partners to build a common understanding of how our adversaries are targeting U.S. networks and critical infrastructure."

The bill tasks CISA with developing clear requirements on exactly what should be reported and by whom. CISA has 24 months to publish a notice of proposed rulemaking in the Federal

Register, but will likely begin promulgating rules much sooner due to the increase in cyberattacks, along with the ongoing conflict between Russia and Ukraine. In the meantime, diligent critical infrastructure operators should begin adjusting incident response plans to increase monitoring and responsiveness in order to ensure compliance with the new requirements.

---

1. The bill references ***Presential Directive 21***, which identifies 16 critical infrastructure sectors.