

Memorandum

TO: U.S. House Representative Tito Canduit — 26th District of Virginia

FROM: Clyde Cabico, Legislative Research Aide

DATE: March 20, 2024

SUBJECT: The Strengthening American Cybersecurity Act of 2022- S.3600

Representative Canduit, as you prepare for your upcoming re-election campaign, you requested a memo summarizing an impactful cybersecurity law that could be highlighted in your outreach to constituents. After reviewing both proposed and recently enacted cybersecurity legislation, I recommend focusing on the Strengthening American Cybersecurity Act of 2022¹, which was signed into law on March 1, 2022.

The Strengthening American Cybersecurity Act of 2022, “ This legislative package, a combination of three bills (the Federal Information Security Modernization Act, the Cyber Incident Reporting Act; and the Federal Secure Cloud Improvement and Jobs Act) focuses on improving cyber incident reporting obligations, “ (ASPR Tracie) requires operators of critical infrastructure and certain other entities to report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA) and/or Department of Homeland Security (DHS) within 72 hours of the incident being detected. It also requires these entities to report any ransomware payments made.

This law is designed to address the large number of cyber-attacks that go unreported every year, limiting the federal government's ability to understand the full scope of the threat landscape and provide timely support. “By mandating detailed reporting for any cyberattack on critical infrastructure, SACA seeks to create a clear view of the threat landscape.” (Center for Digital Government Content Studio) Many companies opt not to report breaches due to concerns over negative publicity, regulatory consequences, or providing information that could be used by competitors. By mandating reporting, “legally mandates operators of critical infrastructure (everything from dams to transportation systems and critical manufacturing),” (Center for Digital Government Content Studio) the government will have a more complete picture of cyber threats, allowing it to quickly render assistance and analyze attack vectors to help other potential victims. Allowing for greater transparency of cyber-attacks from both public and private entities to the government can lead to building robust cybersecurity

¹ For full-text on this bill visit <https://www.congress.gov/bill/117th-congress/senate-bill/3600/text>

strategies in defense, protection, analysis, planning, and incident response and recovery. Title II of the Act focuses on critical infrastructure Sec.201-207.

The ransomware reporting provision is particularly important given the explosion of these kinds of attacks.” Over the past five years, there has been a 256% increase in large breaches reported to OCR involving hacking and a 264% increase in ransomware. In 2023, hacking accounted for 79% of the large breaches reported to OCR. The large breaches reported in 2023 affected over 134 million individuals, a 141% increase from 2022.” (U.S. HHS) For example, in recent years the attacks against critical infrastructure entities like Colonial Pipeline², as well as other organizations like hospitals, schools, and local governments. Tracking ransomware payments provides insights into this lucrative cybercrime business model and can assist law enforcement efforts against ransomware gangs.

While the Strengthening American Cybersecurity Act of 2022 is a step in the right direction, although some potential improvements could be considered:

- a. Instead of 72 hours, tightening the reporting window to 24 hours would enable an even faster response. However, this must be balanced against providing adequate time for covered entities to assess incidents internally first.
- b. Creating a more robust liability shield for entities that report incidents in good faith could alleviate legal concerns deterring some from reporting.
- c. Appropriating additional funding for CISA to adequately manage and analyze the influx of incident reports nationwide.

In highlighting this law to constituents, Representative Tito Canduit, you could emphasize how it will enhance national cybersecurity by ensuring the federal government has the full picture of cyber threats facing our country. Another consideration is that you, Representative Tito Canduit, could give examples of recent high-profile attacks against infrastructure like the Colonial Pipeline breach to illustrate the stakes involved and the vast percentage increase of ransomware attacks as noted previously.

The reporting requirements will drive better information sharing between the private sector and government, empowering a unified defensive posture. “Traditional firewalls and castle-and-moat security strategies that tried to prevent every possible attack are no longer sufficient.” (Center for Digital Government Content Studio) And the ransomware payment reporting will provide transparency into the extortion rackets crippling organizations from hospitals to schools. A unified collaboration to strengthen

² Full report by CISA on the Colonial Pipeline hack that jeopardized critical infrastructure availability on May 7, 2021, by a ransomware attack see— <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>

the defense of information assets between government, private, and public entities is the solution.

Citizens may relate to the increased security provisions aimed at protecting utilities, communications networks, healthcare facilities, and other critical systems that societies rely upon. "In February 2019, Green Ridge Behavioral Health filed a breach report with OCR stating that its network server had been infected with ransomware resulting in the encryption of company files and the electronic health records of all patients." (U.S. HHS) Mentioning this recent event, you could frame the law as the government looking out for the safety and resilience of systems that millions depend on daily.

I, Clyde Cabico, am your Legislative Research Aide, please feel free to let me know if you need any additional information or analysis regarding this cybersecurity legislation as you prepare your outreach campaign. I'm happy to provide additional background and research support.

A handwritten signature in black ink, appearing to be 'Clyde Cabico', with a stylized, flowing script.

Clyde Cabico

Legislative Research Aide

Works Cited

- Easterly, Jen, and Tom Fanning. "The Attack on Colonial Pipeline: What We've Learned & What We've Done over the Past Two Years | CISA." [www.cisa.gov](https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years), 7 May 2023, www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. . Accessed 21 Mar. 2024.
- Rights (OCR), Office for Civil. "HHS' Office for Civil Rights Settles Second Ever Ransomware Cyber-Attack." [www.hhs.gov](https://www.hhs.gov/about/news/2024/02/21/hhs-office-civil-rights-settles-second-ever-ransomware-cyber-attack.html#:~:text=Over%20the%20past%20five%20years), 21 Feb. 2024, www.hhs.gov/about/news/2024/02/21/hhs-office-civil-rights-settles-second-ever-ransomware-cyber-attack.html#:~:text=Over%20the%20past%20five%20years. Accessed 21 Mar. 2024.
- "Strengthening American Cybersecurity Act of 2022- S.3600 | Technical Resources." ASPR TRACIE, asprtracie.hhs.gov/technical-resources/resource/11083/strengthening-american-cybersecurity-act-of-2022-s3600. Accessed 21 Mar. 2024.
- "Text - S.3600 - 117th Congress (2021-2022): Strengthening American Cybersecurity Act of 2022." [Congress.gov](https://www.congress.gov), Library of Congress, 2 March 2022, <https://www.congress.gov/bill/117th-congress/senate-bill/3600/text>.