The Rep. Richmond Cyber Incident Reporting Amendment Needs to Be Rejected by Congress

Forced Reporting and Backdoor Regulation Harm Security and Are Contrary to Voluntary Information Sharing

The U.S. Chamber of Commerce opposes including the Rep. Richmond critical infrastructure incident reporting amendment (CIIRA or the amendment) in the FY 2021 NDAA because of process and policy concerns.[1] The CIIRA needs to be rejected by lawmakers for several reasons.

- **Significant legislation needs to proceed through regular order.** The Chamber has serious concerns with the substance of the CIIRA and the process by which committees of jurisdiction were short-circuited by adding the amendment to the House FY 2021 NDAA (H.R. 6395) without hearings or markups. Industry believes that rushing forward with meaningful legislation such as the CIIRA, which has not been fully vetted through regular order, would be a mistake.

- **Forced reporting undercuts public-private cybersecurity collaboration.** The CIIRA would unravel the consensus that information sharing between industry and the government must be based on collaborative partnerships to work effectively. The amendment would place the private sector in a nonvoluntary relationship with the Department of Homeland Security (DHS) and the federal bureaucracy related to incident reporting, instead of encouraging productive, two-way exchanges of incident data.[2] The business community is concerned about the CIIRA because it would lead to incident reporting by private entities that is compelled rather than voluntary in practice—cutting against the grain of voluntary threat-sharing programs.[3]

- **Rigid incident reporting violates sound cyber risk management.** The CIIRA would require "covered critical infrastructure entities" to report a "covered cybersecurity incident" to the DHS National Cybersecurity and Communications Integration Center within 72 hours. Such an arrangement suffers from a number of flaws, including the following:

    - First, the Chamber is against Congress granting DHS or any agency new rulemaking authority to "establish requirements and a process" tied to mandatory cyber incident reporting by industry. As written, the CIIRA pays insufficient attention to how compliance mandates would drive up costs and misallocate businesses' resources (e.g., human and technical) due to forced reporting.

    - Second, the Chamber rejects policies that would require reporting on a fixed timetable.[4] Among other considerations, what may be understood in the first few days of a cyber incident investigation can be dramatically different from what is learned in the weeks and months that follow.

    - Third, several critical infrastructure sectors (e.g., financial services and energy) have existing legal obligations to report significant cyber incidents to federal and/or state regulatory bodies. It is challenging to discern what increased value would flow to the

federal government when such information is seemingly available to federal agencies. What is more, the CIIRA would interfere with public-private efforts—which already face an uphill climb—to harmonize existing cybersecurity requirements.[5]

- Fourth, discussions with bill writers need to take place regarding a number of provisions (e.g., liability protection), phrases, and definitions, including *covered critical infrastructure entity*, *covered cybersecurity incident*, and *critical infrastructure*.

Businesses share policymakers' goal of mitigating cybersecurity risks and are committing billions of dollars to the security and resilience of their enterprises. The Chamber opposes cyber mandates that are costly, rigid, and potentially duplicative—thus pulling businesses' limited resources away from security and toward compliance. The CIIRA should not be added to the final FY 2021 NDAA. Including it to the defense bill would harm the nimbleness that companies need to both respond to cyber incidents and increase public safety.

(Revised August 14, 2020)

Endnotes

---

[1] See House floor amendment #27/House Rules Committee amendment #625, which is currently section 1637 of H.R. 6395 (PCS version).
https://armedservices.house.gov/_cache/files/f/e/feb65ce0-93fa-4985-8bd4-355238eed8d9/327A5797AA7FBB8010AFE207F75B708C.fy21-ndaa-floor-amendment-tracker-v6.pdf
https://amendments-rules.house.gov/amendments/RICHMO_071_xml713201255525552.pdf
https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395pcs.pdf

The Richmond amendment would implement a recommendation from the Cyberspace Solarium Commission to require the Department of Homeland Security to establish a cyber incident reporting program. See recommendation 5.2.2: Pass a National Cyber Incident Reporting Law. https://www.solarium.gov/report

[2] See, for example, David Turetsky et al., "Success Stories in Cybersecurity Information Sharing," University at Albany, July 15, 2020. https://www.albany.edu/sscis
https://www.lawfareblog.com/cybersecurity-information-sharing-success-stories

[3] See, for example, the Protecting America's Cyber Networks Coalition backgrounder, "Cybersecurity Information-Sharing Legislation: 'Voluntary' Means Voluntary—Separating Fact From Fiction," August 26, 2015. https://www.uschamber.com/sites/default/files/cisa-voluntary-separating-fact-from-fiction.pdf

[4] In comparison with data breach notification legislation, the U.S. Chamber has historically pushed for flexible, not fixed, timing requirements.

[5] See, for example, Senate Homeland Security and Governmental Affairs Committee hearing, "Cybersecurity Regulation Harmonization," June 21, 2017.
https://www.hsgac.senate.gov/hearings/cybersecurity-regulation-harmonization

See, too, the U.S. Chamber's February 2018 letter to the Federal Energy Regulatory Commission regarding the agency's rulemaking, "Cyber Security Incident Reporting Reliability Standards," *Federal Register*, December 28, 2017.
https://www.uschamber.com/sites/default/files/2-26-18_chamber_comments_ferc_cyber_incident_reporting_nopr_final_0.pdf