United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

July 3, 2024

Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, DC 20528-0380

Dear Director Easterly:

I am proud of the bipartisan effort I undertook with U.S. Senator Rob Portman and other Members of Congress in both chambers and on both sides of the aisle to develop and pass the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in March 2022. I also closely followed CISA's progress and rollout of the Notice of Public Rulemaking (NPRM) to implement CIRCIA, issued in April 2024.

CIRCIA is a groundbreaking law, and it was drafted to ensure that critical infrastructure owners and operators report cyberattacks and ransomware payments to the federal government, allowing our nation's cybersecurity agencies to help them respond to and recover from significant attacks and prevent future breaches. It was my intent that this rule would make our critical infrastructure sectors more secure against rising threats posed by foreign adversaries and other attackers and help keep Americans safe.

I recognize that cybersecurity, and particularly cyber incident reporting, is a complex and ever-evolving area. Writing rules for cybersecurity requires hard work and strong collaboration and I know CISA has spent significant time and attention to try to strike the right balance with this rule. However, this regulation will have a huge impact on covered entities, and as I emphasized at my recent hearing on cybersecurity regulatory harmonization, we need regulations that effectively prioritize efforts to strengthen cybersecurity defenses for critical infrastructure, and that do not overburden critical infrastructure owners and operators and pull our cybersecurity professionals away from their mission to focus on compliance. For this reason, it is very important that the regulation is well-crafted and reflects both Congressional intent and the public's recommendations.

As currently written, I have concerns that the effect of this proposed rule would fail to hit this mark. The proposed rule is overbroad and needs additional clarity in the definitions for covered incident, covered entity, and others used in the proposed rule. For example, the definition for covered incident, as written, requires entities to report temporary disruptions to business operations rather than significant disruptions as intended in CIRCIA. CISA has said that it expects to receive 200,000 reports a year, but given the broad definitions, I am concerned that number may be higher CISA's estimate. Under these new requirements, in 2025, thousands of businesses will have to report cyber incidents to the government, and I want to make sure this will not mean that CISA would be able to properly ingest, triage, and analyze the reported information and use the data to improve cybersecurity recommendations and support critical infrastructure.

Additionally, victims of cyber incidents are responsible not just for reporting to CISA, but also making sure other regulators with cyber incident reporting requirements have valid and current sharing agreements or risk compliance violations. The goal of CIRCIA was not to add another long checklist that entities have to adhere to, but to ensure that CISA and the federal government can assist some of our most

critical sectors when they have been the victims of a cyberattack or ransomware incident, to learn from these incidents together, and prevent future incidents. CISA should proactively and earnestly communicate on the status of formulating the information sharing agreements with other federal agencies to ensure that these mechanisms are in place before the final rule is issued and validate that these agreements will be effective mechanisms for improving cybersecurity and supporting the owners and operators of critical infrastructure

CISA needs to meet my and other lawmakers' intent by making the requirements manageable and reciprocal to existing standards and incident reporting requirements by other federal agencies. I strongly encourage CISA to carefully consider public comments from the cybersecurity community, critical infrastructure sectors, and other valuable partners, and re-scope parts of the proposed rule to address these comments.

I request written responses to the below questions within 30 days:

- As a new regulator developing an incident reporting rule for the first time, did CISA consult with other federal agencies while developing the rule?
- Given the Cyber Incident Reporting Council's work to create model incident reporting forms and templates, to what degree were these tools used in formulating the proposed rule? Why did CISA choose to deviate from the CIRC's model?
- Given the discrepancy between the numbers of reports CISA and industry have estimated, how will CISA plan to handle a potential over-reporting of cyber incidents?
- What steps has CISA taken to establish sharing agreements between other federal agencies that have substantially similar reporting requirements? What criteria is CISA using to determine substantially similar incident reporting requirements?

Sincerely,

Gary C. Peters
Chairman
Committee on Homeland Security
and Governmental Affairs