COMMITTEE ON HOMELAND SECURITY

The "Cyber Incident Reporting for Critical Infrastructure Act"
Congresswoman Yvette Clarke (D-NY)

Cyberattacks targeting critical infrastructure (CI) have risen dramatically. Recent attacks like SolarWinds and Colonial Pipeline underscore gaps in existing public-private cybersecurity partnerships, including a lack of clarity about how, when, and why a private CI company should involve the Federal government in responding to a cyber incident. To be a more effective security partner to CI, the Federal government needs to better understand the techniques adversaries are using to carry out cyberattacks so that it is in the best possible position to identify malicious cyber campaigns early and help CI owners and operators defend against future incidents.

Today, most private sector CI are under no obligation to report cyber incidents to *any* Federal agency. As a result, critical security information is not getting to the officials responsible for understanding broader national security consequences and taking action to defend U.S. interests in cyberspace.

As the lead Federal agency responsible for securing CI across all 16 sectors,[1] CISA has: (1) resources and expertise to bring to bear during a cyber incident; (2) established mechanisms for public-private information sharing and interagency collaboration; and (3) institutional knowledge, together with analytic capabilities, to place incidents in a broader context. Currently, the ability for CISA – and the U.S. government as a whole – to effectively partner with the private sector to defend CI networks is hamstrung since it is entirely depends on victim companies voluntarily sharing information about the incident.

Experts inside and outside of government agree that the time has come to require CI owners to report cyber incidents in a centralized, standardized way that helps the Federal government – and in turn, the private sector – understand and prepare for a rapidly evolving cyber threat landscape.[2]

---

[1] See, e.g., Title XXII of the Homeland Security Act of 2002, as amended, Pub. L. 107-296; Sec. 9002 of the National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283; Cybersecurity Act of 2015, Consolidated Appropriations Act 2016, Div. N, Pub. L. 114-113; National Cybersecurity Protection Act of 2014 (Pub. Law 113-282); PPD-21 – *Critical Infrastructure Security and Resilience*, Feb. 12, 2013; PPD-41 – *US Cyber Incident Response Coordination,* July 26, 2016.

[2] See, e.g., Testimony received before the Committee on Homeland Security and Committee on Oversight and Reform, U.S. House of Representatives, hearing entitled *Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign* (Feb. 26, 2021); Testimony received before the Committee on Homeland Security, Subcommittee on Transportation and Maritime Security and Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, hearing entitled *Cyber Threats in the Pipeline: Lessons Learned from the Federal Response to the Colonial Pipeline Ransomware Attack* (Jun. 15, 2021).

The **Cyber Incident Reporting for Critical Infrastructure Act of 2021** would direct CISA to establish requirements and procedures, after robust stakeholder engagement, for certain CI owners and operators ("covered entities") to report certain types of cyber incidents ("covered cybersecurity incidents") to a newly-established Cyber Incident Review Office within CISA.

Specifically, the legislation:

- Directs CISA, after a 270-day period with mandatory windows for stakeholder consultation and comment, to issue an interim final rule setting forth which CI owners and operators are subject to the reporting requirement, which cyber incidents need to be reported, the mechanism for submitting reports, and other details necessary for implementation.

- Tasks the new Cyber Incident Review Office with the discrete mission of receiving, aggregating, analyzing, and securing cyber incident reports to understand adversary trends over time, publishing quarterly reports with anonymized findings, and identifying any actionable threat intelligence that should be shared rapidly and confidentially with cyber 'first responders' to prevent or respond to other attacks.

- Lays out factors and threshold criteria for CISA to use in defining which entities and incidents are covered, but ultimately gives CISA flexibility to tailor the requirements to include only the entities, incidents, and information necessary to inform the Federal government's understanding of the threat landscape and help prevent similar attacks going forward.

- Preserves the integrity of CISA's voluntary partnerships and programs by: 1) directing incident reports to a new Cyber Incident Review Office that is separate and distinct from CISA's voluntary programs; and 2) providing CISA with multiple avenues to obtain information about the incident (instead of traditional regulatory tools such as fines and penalties) that graduates to subpoenaing the information, but only after exhausting other options to bring the entity into compliance.

- Provides multiple protections for reports submitted in accordance with the requirements – both for the reporting *entity* (e.g., liability protections afforded in the Cybersecurity Act of 2015[3]) and the reported *information* (e.g., reports are to be kept confidential and exempt from FOIA) – but would not extend these protections to information obtained through subpoena.

- Ensures that CISA is responsive to the needs of private sector partners – for example, by requiring CISA to notify private sector entities that may have been impacted by data breaches or intrusions on Federal networks, and directing CISA to proactively look for

[3] Sec. 106 of the Cybersecurity Act of 2015, Consolidated Appropriations Act 2016, Div. N, Pub. L. 114-113.

ways to use data on cyber incidents to strengthen private sector security research, consistent with the information protections set forth in the Act.

In short, this bill will give the Federal government crucial visibility needed to bolster the cyber protections of CI, identify malicious cyber campaigns in early stages, identify longer-term threat trends, and make sure actionable cyber threat intelligence is getting to the frontline responders and Federal officials who need it in a manner that also respects confidentiality and privacy.