Introduction

The National Technology Security Coalition (NTSC) is the only national organization representing the Chief Information Security Officer (CISO). As the front-line practitioners who battle cyber threats every day, we believe we offer a unique and critical perspective on cybersecurity.

We believe that the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) is a significant step forward for federal cyber policy, and we thank CISA for its efforts to implement its requirements as quickly as possible. The NTSC is proud to submit the following comments in response to CISA's Request for Information.

1: Definitions, Criteria, and Scope of Regulatory Coverage

The NTSC offers the following feedback regarding some of CIRCIA's definitions:

A. "Covered entity"
   The definition of "covered entity" should ensure commensurate treatment across the various critical infrastructure sectors, which should be held to similar standards of reporting but aligned to the unique characteristics of each sector.

B. "Covered cyber incident"
   The definition of "covered cyber incident" should align as closely as possible to the reporting requirements that already exist from other agencies and reporting frameworks to ensure that the scope of reportable incidents incorporates only incidents that result in actual degradation of critical services and that entities do not have to comply with multiple reporting requirements. We recommend adoption of the definition of "covered cyber incident" found in the Computer Security Incident Notification Rule issued by the Federal Reserve, Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation. That definition is based on National Institute of Standards and Technology (NIST) criteria and stipulate that a reportable incident is one that results in "actual harm" and "materially impacts" a firm's operations.

C. "Substantial cyber incident"
   The definition of "substantial cyber incident" should include only incidents of an elevated severity or effect on the critical infrastructure sector(s). Beginning from the NIST definition of covered cyber incident, the definition of a substantial cyber incident should be elevated such that cyber incidents reported to CISA are not mere technology outages or service interruptions, but rather are incidents so severe as to pose an actual threat to national security, economic security, or public health and safety.

D. "Ransom payment" and "ransomware attack"
   The definition of "ransomware attack" and "ransomware payment" should harmonize as closely as possible with existing definitions from other agencies and reporting frameworks.

E. "Supply chain compromise"
The definition of "supply chain compromise" should be limited to an incident within the supply chain of an information system that (1) an adversary leverages to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and that (2) actually results in a substantial cyber incident.

2: Report Contents and Submission Procedures

A. Reports submitted to CISA by covered entities should not be required to include any information that could potentially disclose specific or technical information about systems, response measures, or vulnerabilities in such detail that would impede a covered entity's response or remediation efforts. Supplemental reports should be required only upon the determination by the covered entity that circumstances surrounding the incident have changed materially.

B. To ensure that covered entities are able to submit required reports during an ongoing cyber event, CISA should establish various alternative means for communicating covered cyber incidents.

C. The 72-hour reporting timeline should begin only upon determination by the covered entity that the incident reaches the substantial cyber incident threshold. Specifically, the definition of "reasonable belief" should be understood to mean that a covered entity has determined in good faith that the incident has reached the defined threshold. The 24-hour timeline for reporting a ransomware payment should begin only upon payment clearance by the covered entity.

3: Other Incident Reporting Requirements and Security Vulnerability Information Sharing

A. CISA should structure its rules in such a way that substantially similar information reported to another federal entity constitutes compliance with CISA's rule.

B. CISA's rules should seek to harmonize reporting timelines and thresholds issued by other federal departments, agencies, and entities.

C. To avoid duplicative reporting while a covered entity is remediating and recovering from an incident, CISA should establish interagency channels to receive information on incidents directly from other federal departments, agencies, and entities.

D. Concerning CISA's request for comments regarding other incident reporting requirements, we respectfully ask CISA to acknowledge and consider the myriad of similar and existing reporting requirements for covered entities who operate in the healthcare, insurance, or financial services industries. Organizations operating in these sectors may be subject to the privacy and data security requirements of the Health Insurance Portability and Accountability Act (45 CFR Part 164) and specific state data breach notification laws. (*See e.g.* International Association of Privacy Professionals, *State Data Breach Notification Chart,* accessed at: State Data Breach Notification Chart [iapp.org]). For example, insurance companies are increasingly subject to additional cybersecurity and notification

requirements under recent state adoptions of the National Association of Insurance Commissioner (NAIC) insurance data security model law, which contains reporting requirements as soon as 72 hours following a cybersecurity event. Multinational organizations have additional requirements to consider, such as those memorialized in the European Union's General Data Protection Regulation, which likewise require 72-hour notification to the appropriate governmental oversight authority. This will impact every commodity vertical across the United States with a mix of existing State and Federal cybersecurity reporting requirements.

4: Additional Policies, Procedures, and Requirements

A. CISA should ensure that its policies, procedures, or requirements related to the enforcement of its reporting requirements reflect the fact that covered entities experiencing cyber incidents are victims of a cyber incident.

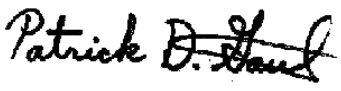
B. CISA should ensure that covered entities are not penalized or subject to enforcement action for reporting pursuant to its rules. CISA's analysis of cyber incident reporting should be structured to help affected parties, and critical infrastructure more broadly, better protect themselves.

C. In the critical period immediately following the discovery of a substantial cyber incident, even the most highly regulated organizations with documented and mature processes for security incident response will be faced with competing, and possibly conflicting, requirements across the state, federal and international regulatory landscapes. In addition to what is noted above, we ask CISA to take into consideration existing laws and frameworks for what constitutes a reportable *covered incident* subject to CIRCIA, such as definitions provided under HIPAA, state-based data breach notification requirements, and similar laws that may already exist for other sectors of critical infrastructure. There will be a formidable burden across CIRCIA's covered entities who must otherwise triage and address requirements and timeframes under conflicting laws.

Conclusion

The NTSC would again like to thank CISA for the opportunity to submit comments on behalf of our CISOs. Cybersecurity is a team sport, requiring the coordination of the public and private sector to match the threats we all face. We look forward to working together to strengthen our collective defense. Thank you.

Sincerely,



Patrick Gaul
Executive Director
National Technology Security Coalition
patrick@ntsc.org