Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

FSSCC Response to the Department of Homeland Security's Request for Comment on the National Cyber Incident Response Plan Update

February 14, 2025

Re: National Cyber Incident Response Plan Update

The Financial Services Sector Coordinating Council ("FSSCC")[1] welcomes the opportunity to comment on the Cybersecurity and Infrastructure Security Agency's ("CISA") proposed update to the National Cyber Incident Response Plan ("NCIRP" or "the plan"). The NCIRP plays a critical role in facilitating an effective national response to significant cyber incidents. A strong and efficient national response to significant cyber incidents not only benefits the member organizations of the FSSCC, but the whole of critical infrastructure.

The FSSCC offers the following recommendations to improve the plan:

The plan should place greater emphasis on the role and capabilities of the private sector.

While the proposed draft improves upon the federal-centric 2016 version of the NCIRP, the plan should go farther and better illustrate the role the private sector plays in a national response. As the owners and operators of much of the nation's critical infrastructure, the private sector plays a vital role in the response mechanism of any incident rising to the level of a "significant cyber incident."[2] The plan, as currently written, focuses first on the coordination efforts of the federal government, referencing the private sector as inputs for federal government outputs. To better illustrate the nation's response capabilities, the plan should place more emphasis on the role and capabilities of the private sector, particularly early in events.

Industries such as the financial services sector have robust response plans and coordination mechanisms. For example, information sharing and analysis centers ("ISACs") serve as central coordination mechanisms for information sharing and response capabilities. In the financial services sector, the Financial Services Information Sharing and Analysis Center ("FS-ISAC") and SIFMA (Securities Industry and Financial Markets Association play a critical role in incident response and coordination that goes well beyond information sharing. Together, with FS-ISAC, SIFMA and the financial services sector are actively engaged in each phase of incident response. While federal coordination makes sense in response to a significant cyber incident, the response plan should underscore the role that the private sector plays outside of its direct coordination with government.

---

[1] The FSSCC is composed of more than 70 financial trade associations, financial market utilities, and the most critical financial firms. The FSSCC coordinates across sector participants to enhance the resiliency of the financial services sector, one of the nation's critical infrastructure sectors. The FSSCC proactively promotes an all-hazards approach to drive preparedness through its collaboration with the U.S. Government for the benefit of consumers, the Financial Services Sector, and the national economy. *About FSSCC*, FSSCC, https://fsscc.org/about-fsscc-13/.

[2] Defined by the NCIRP draft as: "A cyber incident that is (or group of related cyber incidents that together) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."

Consider adding an appendix that demonstrates how existing coordination plans fit into NCIRP.

The draft of the plan undervalues the relationship between the private sector and their Sector Risk Management Agency ("SRMA"), particularly with respect to pre-existing coordination plans. SRMAs play a critical, but often underappreciated role in incident response. For example, the U.S. Department of the Treasury works closely with the private sector participants in financial services throughout all stages of an incident. As a result, the private sector has developed a high level of trust among industry participants and our government partners to come together and collectively defend the sector against cyber threats.

Additionally, private sector industries may have their own response plans that fit into the broader national response mechanisms. For example, the financial services industry has developed the Core Executive Response Group ("CERG"), which serves as a coordinating body for the financial sector to develop an understanding of the scope and scale of an incident or imminent threat, and to assess potential systemic risk. The CERG utilizes the financial sector's partnership with public sector counterparts to coordinate a whole of industry understanding of incidents. Groups like the CERG along with trade associations play key roles throughout incidents which should be captured in the NCIRP.

These coordination efforts, thresholds, and action plans are captured in a number of incident response frameworks and playbooks that collectively outline the sector's response plans to cyber incidents. To best capture the coordinated response capabilities of the private sector and their government partners, the plan should include references to these efforts in Table 6. Additionally, CISA should consider an appendix that demonstrates how these existing coordination plans fit into the NCIRP to ensure the plan captures a more wholistic view of the nation's response mechanisms.

Clarify the role JCDC will play in incident response.

Since the release of the 2016 NCIRP, the structure of federal cybersecurity has shifted greatly, including the creation of CISA and, subsequently, the Joint Cyber Defense Collaborative ("JCDC"). While the FSSCC generally supports CISA's efforts to address cybersecurity risk to the federal government and coordinate with critical infrastructure sectors, we seek greater clarity from CISA over the role of JCDC in incident response. Specifically, FSSCC members have expressed concern with the lack of subject matter experts for various critical infrastructure needs and the lack of information received from JCDC related to potential threats to the sector.

Due to these concerns, FSSCC members remain uncertain about the role that JCDC will play in a significant cyber incident. CISA should update the plan to clarify the role JCDC will play in national coordination and provide guidance as to what the private sector should expect as it relates to information sharing, coordination, and response.

CISA should ensure consistent definitions of a cyber incident.

In the past two years CISA has released multiple definitions of a cyber incident. Most recently, in the notice of proposed rulemaking for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") rulemaking, CISA uses the term "substantial cyber incident." This definition, though similar in name, establishes dramatically different engagement thresholds than the "significant cyber incident" definition used in the NCIRP. FSSCC is supportive of the NCIRP's usage of the PPD-41 definitions for "cyber incident" and "significant cyber incident." We urge CISA to take a unified approach across its authored documents as it relates to a cyber incident to minimize confusion.

Consider adding financial sector resources to Appendix F: Additional Resources.

Appendix F: Additional Resources provides an opportunity for less mature institutions to identify and utilize resources that may help them defend both their own institution and their industry at large. To that end, the FSSCC suggest including FFIEC's Cybersecurity Resource Guide for Financial Institutions as a more comprehensive resource repository.

Conclusion

The FSSCC appreciates the considerable work that went into updating the NCIRP. Maintaining a coordinated national response framework for cyber incidents is critical to our nation's defense in cyberspace. As described above, the FSSCC believes that clarifying the role the private sector plays in this response will create a more holistic view of the complex but coordinated mechanisms at play. The FSSCC welcomes any questions and engagement from CISA as they work to finalize the plan.

Sincerely,

Debbie Guild, PNC Financial Services

FSSCC Chair