U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

March 1, 2023

MEMORANDUM FOR THE CYBERSECURITY ADVISORY COMMITTEE MEMBERS

FROM: Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

SUBJECT: **Formal Response to September 2022 Recommendations**

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) was established in June 2021 to advise, consult with, and make recommendations to CISA on the development, refinement, and implementation of policies, programs, planning and training pertaining to CISA's cybersecurity mission. Since that time, the CSAC has worked to infuse fresh ideas, leveraging its members' significant subject-matter expertise into CISA's cybersecurity mission.

CISA values the hard work of the CSAC that led to a set of actionable recommendations to improve on CISA's execution of its cybersecurity mission. The expert advice and key insights that the CSAC offers will enhance the work of CISA and keep us well-positioned to help address threats in a rapidly changing cybersecurity landscape.

I have worked closely with my leadership team to determine the feasibility of each recommendation and to ensure that we remain within the legal parameters of CISA's operating authorities and resources. Please find CISA's responses to each recommendation as identified in the enclosure; a vast majority of the Committee's recommendations have been accepted and I look forward to implementing them.

Again, I thank the CSAC and its members for your commitment, time, and thoughtful recommendations and look forward to our continued partnership as CISA matures into the Cyber Defense Agency our nation deserves.

Enclosure: CISA's Response to CSAC September 2022 Recommendations

CSAC made the following recommendations related to building resilience and reducing systemic risk to critical infrastructure to the CISA Director:

Note on PPD-21 Rewrite: On November 7, 2022, President Biden notified Congressional leaders that his administration would begin re-writing "Presidential Policy Directive 21 (PPD-21)-Critical Infrastructure Security and Resilience." PPD-21, issued in 2013, details the federal government's approach to detail a "national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure." This rewrite effort will clarify and, as necessary, create new federal policy for: (1) how sectoral, cross-sectoral, and systemic risk is identified, assessed, and managed; (2) the roles and responsibilities of Sector Risk Management Agencies (SRMAs) to manage and respond to risk in their sectors; and (3) CISA's role as National Coordinator to lead the national effort to secure and protect critical infrastructure against the myriad of threats and risks faced by the United States, including the responsibility to define critical infrastructure sectors and designate appropriate SRMAs across the federal government. Therefore, the National Security Memorandum, which may include policies on cybersecurity regulations, systemically important entities (SIEs), and other matters related to managing and prioritizing the nation's risk, which is inclusive of cyber and physical risk, will directly impact how CISA is able to action the following recommendations.

Recommendations 1-5: Identify systemically important entities.

1. Define systemically important entities (SIEs) as "entities with primary responsibility for operating national critical functions (NCFs), whereby an impact on those entities would create systemic risk for the associated NCF."
2. Work with SRMAs, Government Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs) to identify SIEs supporting NCFs relevant to each sector.
3. Modify or replace Section 9 of Executive Order 13636 to accommodate the designation of SIEs tied to an entity's role in operating NCFs. Any policy or law for designating SIEs should include programs for supporting SIE resiliency.
4. Coordinate with SRMAs, GCCs and SCCs to determine how to engage vendors and other third parties that play critical roles in supporting the SIEs' operation of NCFs.
5. Focus national resilience efforts around national security, health and human safety and economic prosperity.

Response: Partially Accept
CISA believes that identifying SIEs is important to prioritize government resources and assets to prevent, mitigate and respond to risks to the most critical entities. During Fiscal Year (FY) 2023, CISA, in close coordination with SRMAs, will work on identifying initial SIEs and develop a program to engage with identified entities.

Estimated Completion Date (ECD): September 30, 2023.

Recommendations 6-7: Develop a common framework for the analysis of systemic risk within NCFs.

6. Work with partners, such as SRMAs and SCCs, to establish a common framework to analyze systemic risk, including a process for decomposing functions, identifying SIEs that support relevant functions and identifying systemic risk transmission channels.
7. Develop a nuanced understanding of each existing function and the primary and enabling entities supporting those functions, and how systemic risk may present itself within each function.

Response: Accept
CISA concurs with the need to standardize, to the extent possible, its approach for assessing systemic risk. CISA is planning to provide risk assessment guidance for sector-level assessments undertaken by SRMAs pursuant to 6 United States Code 665(d) so that the resulting assessments represent the sector risk landscape appropriately while at the same time feeding into the national risk assessments led by CISA. In addition, the National Security Council is currently leading an interagency process to rewrite PPD-21, which will include how the U.S. government identifies and manages systemic risk within and across critical infrastructure sectors.

ECD: September 30, 2023.

Recommendations 8-10: Establish outcome-based national resiliency goals.

8. Work with SRMAs, GCCs, and SCCs to establish a limited number of initial national resiliency goals and create a process for updating these goals on a regular cycle.
9. Establish a Maturity Model with SRMAs and SCCs for enhancing the resiliency of NCFs.
10. Allocate government resourcing – based on priorities set by CISA for government agencies, including SRMAs and SIEs – to support achievement of national resiliency goals.

Response: Partially Accept
SRMAs must prioritize the need for resiliency goals and maturity models in the context of their new statutory responsibilities. Sector-Specific Plans would be an appropriate mechanism through which SRMAs may work with sector partners to socialize and document such goals. CISA is prepared to partner with SRMAs as they seek to establish these goals. During the FY 2023 Appropriations, CISA received funding to establish a SIE Program Office and is in the early stages of its creation. The creation of the SIE Program Office will be done by the Stakeholder Engagement Division in coordination with the National Risk Management Center.

ECD: December 2023.

Recommendation 11: Partner with sectors to establish sector resiliency goals.

11. Engage sectors with SRMAs as full partners throughout the lifecycle of national resiliency efforts, including setting national and sector resiliency goals.

Response: Partially Accept

As the National Coordinator for critical infrastructure security and resilience, CISA believes that partnering with private-sector critical infrastructure owners and operators is imperative to managing risk in critical infrastructure sectors. CISA will take a more active role to build resiliency for critical infrastructure across sectors and continue the interagency process to address key challenges including but not limited to the current sector structure, the wide disparity in capabilities across SRMAs, and needed enhancements to the partnership framework connecting SRMAs with sector partners.

ECD: December 2023.

Recommendations 12-16: Strengthen SCCs and GCCs.

12. Ensure a parity of effort across different sector SCCs, GCCs and their affiliated information sharing and analysis centers and organizations (ISACs, ISAOs).
13. Enhance the effectiveness of GCCs by creating consistent governance structures, including appropriate membership (i.e., to include CISA and other key national security agencies), and with accountability to SRMA cabinet secretaries and agency leadership.
14. SCCs ensure designated SIEs are offered membership in the appropriate SCCs.
15. Leverage sector-led efforts in developing its own work with SRMAs and other government agencies for purposes of national resiliency and incident response.
16. Solicit the Administration, perhaps through the upcoming national cybersecurity strategy, clarifies roles and responsibilities across government agencies with responsibility for national resiliency, including the NRMC and Joint Cyber Defense Collaborative (JCDC) at CISA; SRMAs; regulators; and defense, intelligence, and law enforcement agencies.

Response: Partially Accept

CISA believes that SCCs and GCCs are of prime importance to engaging private-sector partners, sharing information, and promoting resilience efforts. In the FY 2021 National Defense Authorization Act Sec 9002(b) report that CISA produced and that the President approved, CISA has committed to work through the Federal Senior Leadership Council (FSLC) to develop and implement a standardized charter template for GCCs and SCC to ensure high-quality, consistent council performance. CISA is working across several lines of effort—as an SRMA, with the FSLC, and through the Critical Infrastructure Partnership Advisory Council (CIPAC) framework—to optimize both GCCs and SCCs.

ECD: December 2023.

Recommendations 17-21: Establish programs to support national resiliency goals.

17. Engage SIEs and other stakeholders regularly (i.e., every two years) to assess which cybersecurity services (i.e., threat intelligence, network defense tools) are needed from CISA and other government agencies.
18. Leverage the JCDC to facilitate the creation of critical infrastructure support offices that support SIEs and NCFs at intelligence, defense and law enforcement agencies.
19. Collaborate with the Department of Defense to align National Cyber Mission Force teams with the defense of NCFs located within U.S. territory.

20. Collaborate with the U.S. government to assess which resources should be provided directly to SIEs for purposes of meeting resiliency goals.
21. Ensure SIEs meaningfully participate in efforts to meet national resiliency goals, including joining SCCs, ISACs, or ISAOs; engaging with SRMAs; partnering with JCDC; identifying and analyzing systemic risk within relevant NCFs; and, consistent with law, reporting cyber incidents to CISA.

Response: Partially Accept
As the National Coordinator for critical infrastructure security and resilience, CISA retains the statutory authorities to coordinate with SRMAs to manage and mitigate risk and promote resilience within and across critical infrastructure sectors. CISA received FY 2023 Appropriations to establish a SIE outreach program and feedback will be part of the recurring engagements. CISA will leverage national councils, committees, working groups, sector and cross-sector forums, advisory panels, and other relationships to garner feedback on CISA initiatives and to increase understanding of stakeholders' needs and support national resiliency goals.

ECD: December 2023.

Recommendations 22-24: Prevent duplicative regulatory structures.

22. Defer to current regulators for the regulation and supervision of SIEs currently regulated at the federal level and to seek additional authorities where SIEs do not have federal oversight.
23. Promote harmonization of federal regulatory requirements to the NIST CSF.
24. More effectively benefit from regulatory knowledge of NCFs when developing methodologies for analyzing systemic risk and enhancing resiliency.

Response: Partially Accept
CISA believes it is important to reduce duplicative regulatory burdens on regulated entities. CISA will use its requisite authorities and statutory mandates to do so, where feasible and appropriate. However, CISA strongly believes that this harmonization could occur through a common set of regulatory guidelines, which could be informed by the Cross-sector Cybersecurity Performance Goals (CPGs). CISA, therefore, strongly supports the roll-out and adoption of the CPGs by other federal regulators, where feasible and appropriate, and looks forward to working with private-sector partners in developing sector-specific CPGs.

ECD: Ongoing.

CSAC made the following recommendations relating to foreign influence operations and disinformation to the CISA Director:

Recommendation 25: Share information with state and local election officials.

Response: Accept

CISA will continue to work with the intelligence community to ensure that the information needs of election officials around foreign influence operations and disinformation threats are prioritized. CISA will work with the Election Infrastructure Subsector Government Coordinating Council (EIS GCC) and DHS Office of Intelligence and Analysis to identify intelligence requirements. CISA will continue to work with the intelligence community to ensure that intelligence information about adversary activity related to elections is promptly shared as broadly as possible including, where authorized and appropriate, with local election officials. CISA will also continue to provide information on resilience building measures election officials can take to reduce foreign influence operations and disinformation risks to elections.

ECD: Ongoing.

Recommendation 26: Ensure relevant information around foreign hacking and disinformation attacks are shared with the courts, and that the Intelligence Community includes adversary activity targeting the courts in the collection and analysis priorities related to elections.

Response: Partially Accept
CISA will work with the Government Facilities Sector, the Department of Justice and the intelligence community to ensure relevant information around foreign hacking and disinformation attacks are shared with the courts. While CISA can advocate for the courts to be an intelligence community priority, it cannot guarantee the recommendation will be accepted. CISA will also support Government Facilities Sector efforts to increase resilience to foreign influence operations and disinformation within the courts, as appropriate.

ECD: Ongoing.

Recommendation 27: Share up-to-date "best practices" around how to proactively address and counter MDM based on the most recent research.

Response: Partially Accept
CISA's focus on building resilience to foreign influence operations and disinformation is centered on proactively sharing best practices based on the most recent research with partners, including election officials. The most recent example is CISA's Tactics of Disinformation Series in both in English and Spanish in October 2022. This work will continue in 2023 and 2024 through product development, training, and engagement activities. CISA does not, however, provide grants for these activities.

ECD: Ongoing.

Recommendation 28: Ensure that there is a national effort to bring insights together on an ongoing basis, and to share tools, training, and templates.

Response: Accept

CISA will continue to engage partners across government, academia, civil society, and the private sector to ensure insights, tools, training, and templates are available, including on CISA's website.

ECD: Ongoing.

Recommendation 29: Ensure that insights on foreign adversary activity are promptly provided to state and local election officials and consider unique aspects of foreign information operations when developing tools, templates, and training for those officials.

Response: Accept
CISA will continue to follow through on the June 2022 CSAC recommendations it accepted to address foreign influence operations seeking to undermine or disrupt upcoming U.S. elections by building resilience to foreign disinformation that affects U.S. election infrastructure. This includes facilitating information sharing between the intelligence community and election officials on foreign threats to U.S. elections, as appropriate.

ECD: Ongoing.