CISA
CYBERSECURITY
ADVISORY
COMMITTEE

REPORT TO THE CISA DIRECTOR

BUILDING RESILIENCE AND REDUCING SYSTEMIC RISK TO CRITICAL INFRASTRUCTURE

September 13, 2022

Introduction

The Building Resilience and Reducing Systemic Risk to Critical Infrastructure (SR) Subcommittee prepared this report for the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) to advise CISA on how to enhance national resiliency. Focus areas included: identifying systemically important entities (SIEs) responsible for the assets and systems that underpin the National Critical Functions (NCFs); conducting systemic risk analysis with critical infrastructure entities; and establishing effective methods of integrated operational collaboration to reduce cybersecurity risks to NCFs.

CISA provided an initial set of framing questions to guide the Subcommittee's work:

1. How can CISA improve its NCF work and use it to drive national risk management collaboration? How can we best measure reductions of systemic risk? What expectations should CISA set for a scalable analytic model to guide risk prioritization?
2. What is an ideal roadmap for operationalizing primary SIEs? What are the analytic models, timelines, and outputs for such analysis? How should CISA engage with the private sector on such work?
3. What benefits and obligations should accrue to entities identified as systemically important? How would these be operationalized, particularly in the absence of legislation?
4. How can CISA best leverage the Joint Collaborative Environment concept to improve collaborative cyber threat analytics with stakeholders from the public and private sector?
5. How can CISA leverage the power of industry to help defend the nation *in extremis*?

SR addressed these questions through a series of workshops involving participants from critical infrastructure sectors and CISA's National Risk Management Center (NRMC) and Cybersecurity Division. These workshops informed the recommendations contained in this report, which are organized around the three following pillars:

I. Support systemic risk identification to determine SIEs
II. Establish national resiliency goals to drive common analysis and action
III. Create or enhance enabling structures and programs to advance national resiliency

The first pillar is meant to address *who* should be involved in supporting government NCF risk efforts by identifying SIEs. The second pillar addresses *what* these entities and the NRMC seek to achieve around national resilience. The third pillar addresses *how* public and private sector partners should work together to achieve these outcomes.

Findings

SR identified several barriers to improving national risk management, including varying levels of maturity across critical infrastructure sectors, insufficient scope for national resiliency outcomes, and underutilization of existing policy and regulatory approaches that address risk management.

Though the sector-specific approach remains integral to progress, SR identified variation in the collective capability of each sector to support national risk efforts. Without replacing sector-led efforts, CISA and the NRMC have an opportunity to create shared goals and expectations for SIEs in support of NCFs. This will require a phased and iterative approach. For example, after initially determining SIEs, CISA and sector risk management agencies (SRMAs) can then identify the ecosystem of partners that play an integral role in each sector. Since this ecosystem is constantly shifting, CISA should reevaluate SIE designations at an appropriate cadence.

SR repeatedly struggled to address the questions CISA provided without a clear understanding of the desired end state for national risk management. SR believes that a shift toward enhancing national resiliency should reflect current practice within industry and government. For example, the Department of Defense (DoD) has performance goals related to Continuity of Government. SR is unaware of a similar set of national resiliency goals in support of CISA's critical infrastructure mission. The voluntary, cross-sector, common baseline cybersecurity performance goals currently under development by CISA relate to specific cyber control adoption by individual entities.[1] Clear national-level goals in the areas of national security, economic continuity, and health and human safety would help organize public and private critical infrastructure stakeholders in the analysis of what it would take to accomplish those objectives.

SR identified the need for CISA, and its U.S. government partners, to work with stakeholders to identify and provide support or services SIEs may require to enrich national resiliency. As the commercial cybersecurity industry continues to mature, the role of government-provided services will also change, thus requiring CISA to regularly evaluate the value of its service offerings. Certain capabilities (e.g., for intelligence collection, national defense, and law enforcement) will remain unique to the government and should be authorized and resourced in support of critical infrastructure defense.

SR stressed the importance of harmonizing current policy and regulatory approaches that include elements of risk management. Several sectors are already highly regulated, but current national risk management efforts do not sufficiently align with existing policies and regulations. Furthermore, SR stressed the shortcomings of the "Section 9 process," an annual Department of Homeland Security (DHS) requirement to identify and maintain a list of critical infrastructure entities utilizing a risk-based approach, as required by Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*.[2] SR determined that any of CISA's current efforts related to SIEs should replace—not supplement—the Section 9 process and its attendant requirements. Harmonization to existing regulation must be the foundation of any national risk management effort.

Recommendations

Pillar I: Support systemic risk identification to determine systemically important entities – work with sectors to analyze national critical functions and identify key partners in national resiliency.

1. **Identify systemically important entities:** CISA must first identify the entities responsible for operating National Critical Functions to build effective partnerships that enhance national resiliency. CSAC recommends:
    a. CISA defines 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."
    b. CISA works with SRMAs and Sector Coordinating Councils (SCCs) to identify SIEs supporting NCFs relevant to each sector.
    c. Section 9 of EO 13636 should be replaced or modified 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 (see pillar 3).

[1] https://www.cisa.gov/cpgs
[2] https://www.govinfo.gov/content/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

d. Following the identification and designation of SIEs, CISA coordinates with SRMAs and SCCs to consider how to engage vendors and other third parties that play critical roles in supporting the SIEs' operation of NCFs.

e. CISA scopes national resilience efforts around focus areas like national security, health and human safety, and economic prosperity. This would enable CISA to use resources and personnel more efficiently to prioritize the appropriate NCFs--and SIEs--and orient national resilience programming within each scope. For emerging risk, strategic risks, and operational response, it is important to prioritize the NCFs and SIEs whose failure is most likely to cause cascading impacts with significant consequences by focus areas. These focus areas would also determine the scope of the cross-sector efforts described in recommendation 5a.

2. **Develop a common framework for the analysis of systemic risk within NCFs:** Understanding systemic risk within each NCF is foundational towards enhancing the resiliency of each function and the country as a whole. While unique methodologies may be necessary to understand systemic risk within each function, a common framework for approaching systemic risk analysis would create shared terminology and enable the understanding of cross-function risk. Gaining high level understanding of all NCFs is a greater priority at this point than understanding cross-sector risks. CSAC recommends:

   a. CISA works 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.[3] CISA's goal should be to create a methodology that can be documented, validated, and deployed in a common, repeatable fashion across sectors, which enables SRMAs and SCCs to account for sector-specific features, dependencies, or models in the methodology's implementation.

   b. CISA develops 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. **SR believes the current focus on measuring large-scale systemic risk, risk across functions, or scalable models for national risk is premature.** Likewise, overly specific analysis of sub-functions is a lower priority than forming an initial understanding of primary functions. Cross-sector analysis can only be pursued once a common battle rhythm has been achieved in multiple sectors and functions.

Pillar II: Establish national resiliency goals to drive common analysis and action – develop a shared approach among SIEs and government agencies for enhancing the resiliency of NCFs.

3. **Establish outcome-based national resiliency goals:** Common goals should establish the shared outcomes that SIEs and government partners seek to achieve and focus collective action. CSAC recommends:

   a. CISA works with SRMAs and SCCs to establish a limited number of initial national resiliency goals and create a process for updating these goals on a regular cycle. Initial resiliency goals could include establishing common frameworks for analyzing systemic risk (rec. 2), creating, and maintaining baseline security and resiliency risk management approaches (i.e., CISA performance goals), building integrated resiliency planning and defense, and developing metrics for evaluating resiliency.

   b. In developing the national resiliency goals, CISA establishes a Maturity Model with SRMAs and SCCs for enhancing the resiliency of National Critical Functions.

   c. Allocate government resourcing – based on priorities set by CISA for government agencies, including SRMAs and SIEs – to support achievement of national resiliency goals.

[3] An example of an analytical framework for evaluating systemic cyber risk within and across sectors: https://sipa.columbia.edu/sites/default/files/CRFS%20Working%20Paper%20The%20Ties%20that%20Bind.pdf

4. **Partner with sectors to establish sector resiliency goals:** Critical infrastructure owners and operators are ultimately responsible for managing risk to NCFs. These owners and operators, working at the sector level, should help define national resiliency goals and drive the processes and outputs of risk analysis, with the support of CISA and SRMAs. Individual sectors should form common resiliency goals to focus public-private efforts to protect NCFs operated or supported by the sector. CSAC recommends:
    a. CISA engages sectors with SRMAs as full partners throughout the lifecycle of national resiliency efforts, including setting national and sector resiliency goals.

Pillar III: Create or enhance enabling structures and programs to advance national resiliency goals – enhance current public-private partnership structures and evolve authorities and capabilities to support national resiliency efforts.

5. **Strengthen SCCs and Government Coordinating Councils (GCCs):** The SCCs and GCCs can be a highly effective structure for facilitating public-private collaboration on operational and policy matters. CSAC recommends:
    a. CISA, along with SRMAs, GCCs and SCCs, ensures a parity of effort across different sector SCCs, GCCs, and their affiliated information sharing and analysis centers and organizations (ISACs, ISAOs). SCCs and GCCs can more effectively collaborate with each other to find commonalities and drive prioritization of national efforts. This mechanism would yield an organic prioritization of the NCFs and allow CISA to operationalize specific mission spaces. CISA should facilitate purpose-specific, cross-sector engagements, which might be necessary to support the achievement of national and sector resiliency goals. CISA should augment the existing Cross-Sector Coordinating Council under the Critical Infrastructure Partnership Advisory Council (CIPAC) structure,[4] with multiple, cross-sector groups scoped to address specific issues or adverse impact scenarios and invite appropriate and relevant SCC members and their designees to coordinate on these issues. The Tri-Sector Executive Working Group (comprised of the finance, energy, telecommunications sectors) is a good example of the benefits derived from a collaborative, purpose-specific initiative across sectors.[5]
    b. CISA, with SRMAs, enhances 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. Sectors view the GCCs as the primary means for engaging the U.S. government on matters of national security and critical infrastructure resiliency, but the GCCs are often uncoordinated or lack agency representation to help elevate issues to the leadership level.
    c. SCCs ensure designated SIEs are offered membership in the appropriate SCCs.
    d. CISA *leverages* sector-led efforts in developing its own work with SRMAs and other government agencies for purposes of national resiliency and incident response. Some sectors have created self-organized ISAOs designed to analyze systemic risk and collaborate on associated threats. Government has struggled to integrate the output of such organizations into its' own efforts, leading to inefficiencies and duplication of efforts.
    e. 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. Updating CISA's National Infrastructure Protection Plan[6] and other policies to clearly reflect the role that each organization plays is crucial to effectively communicating processes and procedures to private sector stakeholders.
    CISA increases communication with stakeholder groups beyond Chief Information Security Officers. Engagement with Chief Information Officers and other senior executives at SIEs can help inform

[4] https://www.cisa.gov/critical-infrastructure-partnership-advisory-council
[5] https://www.cisa.gov/tri-sector-executive-working-group
[6] https://www.cisa.gov/national-infrastructure-protection-plan

strategic understanding of risks, facilitate high-level exchanges on threats, and drive prioritization of national resiliency goals.

6. **Establish programs to support national resiliency goals:** There needs to be a collective reimagining of the relationship between the U.S. Government and critical infrastructure as one of shared obligations for national resiliency. SIEs have responsibility for managing risk within their organization and should be expected to take reasonable action to mitigate systemic risks to national resiliency. CISA and the U.S. government should understand the needs of SIEs and ensure the necessary capabilities and programmatic support are made available. Compelling programs that provide needed support will motivate active partnerships. CSAC recommends:
    a. CISA engages 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. As part of this engagement, CISA should seek to understand barriers to access such services, including lack of availability or high cost. CISA should evaluate whether it needs to develop or offer services directly or if it should provide funding vehicles (i.e., grants, tax credits) that enable provision of commercial solutions. CISA should discontinue current service offerings when it finds little stakeholder demand.
    b. CISA leverages JCDC to facilitate the creation of **critical infrastructure support offices that support SIEs and NCFs at intelligence, defense, and law enforcement agencies**. These support offices should be resourced to provide partnership with SIEs and NCFs and ensure that all necessary authorities and capabilities are being leveraged in defense of critical infrastructure. IC, DoD, and LE participation in the SCCs and GCCs could further deepen understanding and partnership with the critical infrastructure community (rec. 5).
    c. **CISA collaborates with the DoD to align National Cyber Mission Force teams with the defense of NCFs located within U.S. territory.** These teams should conduct contingency planning, drills, and joint responses with SIEs operating NCFs, to not only ensure the defense mission but also the resiliency of the Nation. These efforts should be integrated with the Federal Emergency Management Agency and its authorities for managing response for events with physical impact.
    d. U.S. government assesses which resources should be provided directly to SIEs for purposes of meeting resiliency goals. Not all SIEs will be private companies operating in competitive markets with the ability to dedicate resources towards enhancing resiliency and partnering to reduce systemic risk. Some SIEs will be government or nonprofit organizations, or companies operating in markets with fixed cost-structures. In these situations, the U.S. government should offer funding and other resources to promote national resiliency.
    e. 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.[7] This recommendation is reliant upon action under recommendation 5, which encourages SIEs to join SCCs. If an SIE is not resourced to meaningfully participate, it should contact CISA and its SRMA for support.

7. **Prevent duplicative regulatory structures:** Many SIEs (i.e., those in finance, energy, health care, telecommunications, etc.) are already regulated at the Federal level, including for cybersecurity and resiliency practices. CISA should prevent the imposition of duplicative regulatory regimes which will likely be conflicting and ineffective. CISA can most effectively raise cybersecurity standards across regulated sectors by promoting the use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) as a baseline for regulatory expectations. CISA should work with Congress to create appropriate regulatory oversight for those SIEs not already federally regulated for cybersecurity. CSAC recommends:

[7] Division Y of Public Law 117-103, the Consolidated Appropriations Act, 2022," includes the Cyber Incident Reporting for Critical Infrastructure Act of 2022:" https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf.

a. CISA defers 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. CISA performance goals should not be imposed as additional regulatory expectations.

b. CISA promotes harmonization of Federal regulatory requirements to the NIST CSF. As CISA develops performance goals, it should utilize a risk-based approach and avoid compliance checklists that "cherry-pick" individual controls at the expense of comprehensive risk management practices.

c. More effectively benefit from regulatory knowledge of NCFs when developing methodologies for analyzing systemic risk and enhancing resiliency.

Conclusion

SR will continue to research, refine the recommendations, and prepare the recommendations for adoption in case CISA approves them. Furthermore, the foundational effort outlined in the recommendations would provide better insights into how Joint Collaboration Analysis as well as Operational Collaboration might need to play out *in extremis*.

Acknowledgement

The Subcommittee would like to thank the subject matter experts who supported and worked on this initiative:

Jeff Baumgartner, Berkshire Hathaway Energy
Kathryn Condello, Lumen
Brett DeWitt, MasterCard
Ben Flatgard, JPMorgan Chase
Michele Guido, Southern Company
Scott Jones, Johnson & Johnson
Stacy O'Mara, Mandiant
Katheryn Rosen, JPMorgan Chase
Claire Teitelman, JPMorgan Chase
Pat Turchick, Johnson & Johnson

Also, special thanks to CISA staff and private sector representatives who participated in the workshops.