CISA CYBERSECURITY ADVISORY COMMITTEE

REPORT TO THE CISA DIRECTOR

Building Resilience and Reducing Systemic Risk to Critical Infrastructure

September 13, 2023

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established a Building Resilience and Reducing Systemic Risk to Critical Infrastructure (SR) subcommittee (hereinafter referred to as the "Subcommittee") to enhance national resiliency.

Previous recommendations were organized around three pillars:

I. Analyze systemic risk to identify systemically important entities.
II. Establish national resiliency goals to drive common analysis and action.
III. Create or enhance enabling structures and programs to advance national resiliency.

In a formal response letter from CISA Director Easterly to the CSAC on March 1, 2023, Director Easterly stated recommendations (in support of the three pillars) were either "Accepted" or "Partially Accepted." These recommendations are fundamental and foundational to the collective capability of each sector to support national risk efforts.

In March 2023, CISA provided a new tasking document to the CSAC, outlining three areas of study. The CISA National Risk Management Center (NRMC) is interested in reducing risk to critical infrastructure and measuring the efficacy of their role in doing so. The Subcommittee was tasked to provide a critical infrastructure perspective to inform these efforts.

The Subcommittee tasking document also included the following tasking questions to guide the Subcommittee's work:

1. How can the governance, processes, and analysis in CISA's National Critical Infrastructure Risk Register create the greatest opportunity for risk reduction?
2. What risk information would help private sector entities, especially systemically important entities (SIEs), plan and execute risk reduction measures?
3. How can CISA incentivize close collaboration between SIEs and the U.S. government on their security and resilience?

Findings

The Subcommittee members conducted a series of meetings to ensure that CISA's Joint Cyber Defense Collaborative (JCDC), National Risk Management Center (NRMC), and Stakeholder Engagement Division (SED) are aligned on work concerning critical infrastructure. Special topical meetings included NRMC's SIE criteria and methodology, the SED's SIE Outreach Initiative, and evaluation of Space as an independent sector.

The Subcommittee members agreed that its work would focus on architecture and capabilities to optimize collaboration between the critical infrastructure and the U.S federal government, as well as a reimagination of the public-private partnership for national security, risk, response, and resilience.

To understand the current landscape of operational collaboration, the Subcommittee members conducted a series of sector-specific engagements across seven sectors/subsectors.

1. Energy (electricity, oil and natural gas, dams, nuclear)
2. Finance
3. Communications
4. Transportation (railways, airlines, shipping, trucking)
5. Healthcare
6. Water
7. Chemical

The goal of these engagements was to solicit feedback on how the federal government—especially, but not exclusively, CISA's NRMC, SED, and JCDC—can most effectively collaborate on national security, critical infrastructure protection, and risk management issues with critical infrastructure owners and operators, associated vendors, and other stakeholders. The engagements addressed the following topics:

- The appropriate mix of stakeholders with which the federal government can engage when seeking private sector input on national security, critical infrastructure protection, and risk management activities and policies (e.g., Sector Coordinating Councils, Information Sharing and Analysis Centers, Section 9-designated entities, state and local government entities and international partners);

- The venues and mechanisms through which the federal government should engage such stakeholders (e.g., the role of Sector Risk Management Agencies (SRMAs), the NRMC, SED SIE Outreach Initiative, JCDC, and other government-, industry- and public-private bodies); and

- Strategic and long-term goals for federal government consultation with critical infrastructure owners and operators (e.g., how industry-specific mechanisms and exchanges can be leveraged to provide sustained support for such efforts, integration with other elements of government, such as intelligence and law enforcement entities, and how to facilitate cross-sector engagement in such efforts).

The Subcommittee members considered what attributes a sector (or other organizing function) might require for effective operational collaboration. In developing the attributes for architecture for operational collaboration, they referenced the New York Cyber Task Force's definition of Operational Collaboration as, "the integrated public-private preparation and response to severe cyber crises"[1]:

In response to the Subcommittee's taskings regarding the optimization of governance, processes, and analysis within CISA's National Critical Infrastructure Risk Register, comprehensive insights are provided. These insights are aimed at fostering risk reduction, enhancing collaboration, and establishing a robust feedback loop/cycle with the private sector, particularly SIEs, to build a more resilient critical infrastructure landscape.

There are three critical attributes for the architecture of a sector's operational collaboration model.

1. Risk Analysis and Mitigation - Enables a deeper understanding of how systemically important functions (i.e., National Critical Functions (NCFs)) operate, including business and technical underpinnings, as well as national security impact of compromise.

2. Illumination of the Battlefield - Drives a risk-informed intelligence collection and analysis apparatus that integrates the capabilities and accesses of private sector and government organizations. Provides early warning capability of

[1] https://www.sipa.columbia.edu/sites/default/files/2023-02/NYCTF%202020%20Operational%20Collaboration-report.PDF

adversary intent/capability.

3. Integrated Response - Enables government and critical infrastructure to respond to an event by collaborating and sharing information about attacks and risk mitigating actions to change the trajectory of our country's and industry's collective defense, response, and resilience.

The tactical elements that can produce an effective architecture and capabilities include:

- Government and private sector convening structures that are integrated and enable collaboration among different peer groups (i.e., CEO, CIO, CISO, COO, operations, risk management, incident response, etc.). Use of existing convening structure that is CEO-connected at minimum, if not led (Sector Coordinating Councils (SCCs), Information Sharing and Analysis Centers (ISAC), Section 9, the President's National Security Telecommunications Advisory Committee (NSTAC), etc.);
- Integration of steady state policy coordinating bodies with purpose-built incident response entities.
- Section 9 and/or SIE–specific organizations that are integrated with broad-based sector-wide collaboration centers.
- Clear collaboration and throughput between:
    - Private sector: owners/operators (i.e., firms), industry associations, collaboration centers (e.g.., ISAC, Analysis and Resilience Center for Systemic Risk (ARC), Department of Energy's Energy Threat Analysis Center (ETAC) etc.), and SCCs
    - Government: Department of Defense, law enforcement, Intelligence Community (IC), CISA/DHS, SRMAs, Government Coordinating Councils (GCC)
- Focus of the convened group should be consistent with national security objectives (e.g., for alignment with CISA's NRMC and JCDC, and FEMA) and address the following questions:
    - Is there credibility with SRMAs; is the appropriate level at table from Federal government? (Example Deputy Secretary or higher)
    - Is convening structure sustainable and adaptable;
    - Able to avoid duplication or pancaking layers of regulation;
    - Able to assess interdependencies and 1st, 2nd, 3rd derivative issues, including supply chain;
    - Able to integrate with:
        - SRMA
        - IC; FBI, US Cyber Command, Secret Service, National Security Agency, Office of the Director of National Intelligence
        - Department of Defense, Federal Bureau of Investigation, Secret Service
        - Other private sector critical infrastructure participants/interdependencies
        - State, Local, Tribal, Territory (SLTT)
        - International

Recommendations

- With respect to recommendations identified in September 2022, implementation of recommendations is underway and should be consistent with outcome of the PPD-21 Rewrite. CISA should not proceed with SIE designations until it collaborates with private sector regarding existing critical infrastructure designations and authorities (i.e., EO 13636 Section 9).

- CISA should develop an ongoing process for reviewing attributes and maturity model for achieving operational collaboration. The process should be managed by CISA with sector-led implementations conducted by SRMAs/GCCs and SCCs. This maturity model would create a pathway for both industry and government capabilities to progress in an organized and coordinated fashion that is accountable to scrutiny.

- CISA should more clearly define their role as National Coordinator with supporting architecture and an organizational structure. This structure should include defined SRMA roles, responsibilities, and capabilities. At a minimum, CISA should ensure sector-specific points of contacts for ease of integration by non-CISA personnel (SRMAs and Sectors/Subsectors).
    - This recommendation also supports the White House National Cybersecurity Strategy implementation plan 1.2.5 tasking of "Establish an SRMA Capability".
    - See Appendix A SRMA ANNEX as a template example.

- CISA, as the lead agency responsible for the White House National Cybersecurity Strategy implementation plan 1.4.1 tasking "Update National Cyber Incident Response Plan" (NCIRP), should develop an owner/operator-centric update to the NCIRP. Rather than considering what government needs to support its decision making and efforts, it should use a first-principles approach to considering how the government can support owners/operators during crisis.
    - The NCIRP update should also align to FEMA's incident response plan. CISA should include the critical infrastructure asset owners and operators as part of the tasking team.

- The National Critical Infrastructure Risk Register exemplifies CISA's commitment to bolstering our national security. To maximize the potential for risk reduction, CISA must refine the governance structure to encompass designated critical infrastructure private sector representatives. CISA should establish dedicated working groups—where public and private experts collaboratively engage in risk analysis—to ensure comprehensive insights that effectively mirror real-world scenarios. Additionally, recognizing the pivotal role of SCCs, CISA should encourage these councils to integrate experts to address intricate risk scenarios in support of a national risk strategy.

- To the extent that sectors/subsectors have already developed a risk register, CISA and SRMAs should align their own efforts with industry approaches where possible and appropriate.

- CISA's collaboration with SRMAs has proven instrumental but needs improvement. To operationalize the aggregate efforts and effectively diminish risk, CISA's NRMC should engage in regular collaboration with the critical infrastructure private sector. This engagement should extend to promote systemic interaction with CISA's JCDC, the SCCs, GCCs, and SRMAs—ensuring all stakeholders with relevant expertise are at the decision-making table and have common operating picture across sectors. This recommendation is stated without insights from the SIE beta list or the National Critical Infrastructure Risk Register currently under development at CISA. These were never shared with the Subcommittee.

- Architecture from both the private and public sector for operational collaboration will form a sustaining approach. CISA should explore ways to establish a standing, private sector CEO-led Committee that would report directly to the President of the United States, with participation from the Office of National Cyber Director, National Security Council, CISA Director and the Homeland Security Advisor, to ensure that resilience—including continuity planning-- is a priority. The function of this Committee would be to support the Continuity of the Economy through exercises with Cabinet-level members.

Conclusion

Consistent with Cyberspace Solarium Commission recommendations, the heart of this work has been to operationalize the proposed collaboration between the private sector and the federal government. The recommendations provided above seek to illustrate this constructive collaboration. Much work is underway and should be noted that this needs to be an evergreen evaluation.

Appendix A: List of Contributors to this Report

The following SR subcommittee members participated in the study and recommendations documented in this report.

Tom Fanning, Subcommittee Chair, Southern Company
Marene Allison, Former Johnson & Johnson
Lori Beer, JPMorgan Chase
Rahul Jalali, Union Pacific
Jim Langevin, Former U.S. House of Representatives
Cathy Lanier, National Football League
Kevin Mandia, Mandiant
Suzanne Spaulding, Center for Strategic and International Studies
Alicia Tate-Nadeau, Illinois Emergency Management Agency

APPENDIX B — Sector Risk Management Agency (SRMA) Energy Annex
(Recommendation 3 template example)

Sector Risk Management Agency:	Support Agencies:
Department of Energy	Department of Homeland Security Department of Transportation Department of Defense Department of Justice Office of the Director of National Intelligence Office of the National Cyber Director Federal Energy Regulatory Commission

INTRODUCTION

Purpose
[same across SRMAs – outlines purpose of SRMAs generally and the purpose of each annex]

Scope
The term "energy" includes producing, storing, refining, transporting, generating, transmitting, conserving, building, distributing, maintaining, and controlling energy systems and system components. The sector includes the electricity, oil, and natural gas subsectors but excludes the hydroelectric and commercial nuclear power facilities and pipelines. [additional information defining the scope of the sector]

CROSS-SECTOR DEPENDENCIES

This section describes how the energy sector supports and relies on other critical infrastructure sectors.

Transportation Systems Sector
The energy sector's heavy reliance on pipelines to distribute products across the nation highlights the interdependencies between the energy and transportation systems sectors. The transportation systems sector is also designated a lifeline function, meaning its reliable operation is so critical that a disruption or loss of function will directly affect the security and resilience of other critical infrastructure sectors, including energy. The dependencies are reciprocal: the transportation systems sector is dependent on the energy sector for fuel to operate transport vehicles and power for overhead transit lines. Within the energy sector, transportation electrification is shifting the dependency away from the oil and natural gas subsector toward the electricity subsector.

Communications Sector
Both the energy sector and the communications sector provide lifeline functions, meaning they are highly interdependent. The communications sector relies on the energy sector for fuel to maintain temperatures for equipment and to provide backup power and energy to run cell towers and other transmission equipment. In turn, the energy sector is dependent on the communications sector to perform many monitoring and control functions, including breakage and leak detection and remote control of operations on the oil and natural gas side and the detection and maintenance of operations and electric transmission on the electricity side.

Water Sector
The energy sector's reliance on water stems from the importance of water in production operations for both the electricity and natural gas subsectors and the use of water as a coolant in many power generation facilities. Water treatment plans rely on the energy sector for fuel and electric power to operate pumps and treatment plants.

Information Technology Sector
Increasing cyber and information technology dependencies have created new and evolving risks for the energy sector.

Energy control systems and the information and communications technologies on which they rely play a key role in North American energy infrastructure. These cyber and information technology components are essential in monitoring and controlling the production and distribution of energy.

Critical Manufacturing Sector

Concerns about the availability and security of critical energy sector goods and components sourced from adversary nations have exacerbated supply chain constraints facing the energy sector. The energy sector relies heavily on the domestic critical manufacturing sector to provide materials like large power transformers, semiconductors, solar photovoltaics, and other key inputs to energy systems and processes. Long lead times for key operational equipment can create reliability and security concerns for the sector by stressing the ability of critical infrastructure owners and operators to respond to natural disasters and man-made threats.

Other Sectors and Dependencies

Given that energy infrastructure provides essential fuel and power and provides one of the four lifeline functions, all other critical infrastructure sectors experience interdependency with the energy sector. Shared dependencies on the providers of the other three lifeline functions also create risks for the energy sector. Geographic co-location can also create interdependencies between critical infrastructure owners and operators, and sector risk management agencies should account for the geographic placement of critical infrastructure facilities when scoping cross-sector risk management activities. In addition to cross-sector dependencies, the energy sector is characterized by dependencies between the natural gas and electricity subsectors. Natural gas is used for electric generation, yet constrained infrastructure to deliver natural gas supplies to power generators in certain locations create reliability issues. The natural gas subsector also depends on electricity at production, pipeline, processing, and distribution facilities.

CORE CAPABILITIES AND ACTIONS

As described in Presidential Policy Directive 21 and U.S. Code at 6 U.S.C. § 665d, national infrastructure security is built on a partnership between government and private industry that combines the implementation of policy, regulatory, and voluntary actions to manage risk. Both public and private entities own and operate the nation's critical infrastructure, but the risk associated with the destruction or failure of that infrastructure is borne by a much larger population of Americans—and disproportionately by vulnerable or disadvantaged communities and people of color. For this reason, the effort to secure the nation's critical infrastructure requires a whole-of-government approach and coordination and collaboration across multiple intergovernmental and industry stakeholders. This section outlines the core capabilities, as identified by the CISA's list of National Critical Functions, that the energy sector supports and specifies the responsibilities of the sector risk management agency and each supporting agency.

Energy Sector Alignment with National Critical Functions

National Critical Function	Energy Sector
Generate electricity	
Transmit electricity	
Distribute electricity	
Exploration and extraction of fuels	
Fuel refining and processing fuels	
Store fuel and maintain reserves	
Provide material and operational support to defense	
Provide and maintain infrastructure	

Agency Functions

Sector Risk Management Agency	Functions
Department of Energy (DOE)	**Support sector risk management** • Establish and carry out programs to assist critical infrastructure owners and operators within the energy sector and its subsectors in identifying, understanding, and mitigating threats, vulnerabilities, and risks to energy systems or assets. • Recommend security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets. **Assess sector risk** • Identify, assess, and prioritize risks within the energy sector and its subsectors, considering physical security and cybersecurity threats, vulnerabilities, and consequences. • Support national risk assessment efforts led by the Department of Homeland Security. • Participate in planning efforts related to the revision of the *National Infrastructure Protection Plan* and the development and revision of the energy sector-specific plan.

	Sector coordination • Serve as day-to-day federal interface for the prioritization and coordination of sector-specific activities and responsibilities. • Serve as the federal GCC for the energy sector and facilitate interagency, intergovernmental, and cross-jurisdictional coordination on issues affecting the energy sector as they pertain to critical infrastructure security and resilience. • Participate in cross-sector coordinating councils, including the Federal Senior Leadership Council. **Facilitate information-sharing** • Facilitate access to and exchange of information and intelligence necessary to strengthen the security of energy sector critical infrastructure, including through the Electricity-ISAC and the ETAC. • Facilitate the identification of intelligence needs and priorities of energy sector critical infrastructure owners and operators in coordination with the Director of National Intelligence. • Support DHS reporting requirements by providing energy sector-specific critical infrastructure information. **Support incident management** • Support incident management and restoration efforts during or following a security incident. • Support the CISA Director in national cybersecurity asset response activities for critical infrastructure. **Contribute to emergency preparedness efforts** • Coordinate with energy sector owners and operators and the CISA Director in the development of planning documents for coordinated action in the event of a natural disaster, act or terrorism, or other man-made disaster or emergency. • Participate in, conduct, or facilitate exercise and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the energy sector. • Support the Department of Homeland Security and other federal departments and agencies in developing planning documents or conducting exercise or simulations when relevant.

Support Agency	Functions
Department of Homeland Security (DHS)	**Cybersecurity and Infrastructure Security Agency** • Execute roles and responsibilities—including partnership management; planning, analysis, and reporting; capacity building; information sharing; and incident management—as National Coordinator through the Federal Senior Leadership Council. (per the 9002 (b) report) • Ensure a unified approach to risk management across critical infrastructure sectors. • Facilitate the development of standardized methodologies for assessing the maturity and effectiveness of sector-specific partnership structures. • Maintain and periodically facilitate a process for updating the sector-specific annexes outlining SRMA roles and responsibilities. • Maintain the National Coordinator assistance model to outline the provision of CISA resources to SRMAs for enhanced coordination and technical support for sector-level risk analysis. • Receive and analyze sector-specific information provided annually by SRMAs to identify opportunities for cross-sector collaboration on risk management activities. • Work with the Office of the National Cyber Director to engage the Office of Management and Budget to identify budgetary requirements for energy sector risk management activities. • Operate the Joint Cyber Defense Collaborative and coordinate energy sector-specific operational collaboration activities with the Energy Threat Analysis Center. **Transportation Security Administration** • Support risk assessment and management activities as they relate to pipelines serving energy infrastructure. **Federal Emergency Management Agency** • Provide oversight of emergency preparedness activities carried out under ESF #12. • Maintain the National Response Framework or its successor as the organizing concept for emergency preparedness and disaster response efforts.
Department of Transportation (DOT)	**Pipelines and Hazardous Materials Safety Administration** • Support risk assessment and management activities as they relate to pipelines serving oil, natural gas, and other energy infrastructure. • Develop and implement safety regulations and guidance for pipelines, underground natural gas storage, and liquified natural gas facilities.
Department of Defense (DOD)	• Operate, defend, and ensure the resilience of all DOD-owned or contracted critical infrastructure. • Secure national security and military systems. • Investigate criminal cyber activity under military jurisdiction.

Department of Justice (DOJ)	Federal Bureau of Investigation • Lead counterterrorism and counterintelligence investigations and related law enforcement activities. • Conduct domestic collection, analysis, and dissemination of cyber threat information. • Operate the National Cyber Investigative Joint Task Force.
Office of the Director of National Intelligence (ODNI)	• Use applicable authorities and coordination mechanisms to provide intelligence assessments regarding threats to critical infrastructure and coordinate intelligence and other sensitive or proprietary information related to critical infrastructure. • Oversee information security policies, directive, standards, and guidelines for safeguarding national security systems.
Office of the National Cyber Director (ONCD)	• Work with the Cybersecurity and Infrastructure Security Agency to engage the Office of Management and Budget to identify budgetary requirements for energy sector risk management activities.
Federal Energy Regulatory Commission (FERC)	• Facilitate the exchange of information with critical infrastructure owners and operators during incident response and recovery. • Encourage critical infrastructure owners and operators to participate in public-private partnerships. • Ensure sector resilience through policymaking and oversight.

Other Stakeholder Functions

Stakeholder	Functions
Systemically Important Entities	• Participate in national risk management activities through the Electricity Subsector Coordinating Council and/or the Oil and Natural Gas Subsector Coordinating Council. • Undertake internal activities and engage in sector and cross-sector activities to conduct risk assessments, understand dependencies and interdependencies, develop and coordinate emergency response plans, establish continuity plans and programs, participate in training, and exercise activities, and contribute technical expertise to critical infrastructure security and resilience efforts. • Adhere to industry best practices and comply with all applicable laws and regulations regarding security practices.
Electricity Subsector Coordinating Council	• Serve as the electricity subsector policy coordination and planning entity to collaborate with DOE as the SRMA and chair of the GCC. • Represent principal entry point for the government to collaborate with the electricity subsector for critical infrastructure security and resilience activities. • Serve as a strategic communication and coordination mechanism between owners, operators, suppliers, and, as appropriate, the government during emerging threats or response and recovery operations. • Participate in planning efforts related to the revision of the *National Infrastructure Protection Plan* and the development and revision of the energy sector-specific plan. • Review the annual submission to DHS on electricity subsector activities. • Understand and communicate requirements of the subsector for government support. • Provide input to the government on research and development efforts and requirements for the electricity subsector.

Oil and Natural Gas Subsector Coordinating Council	• Serve as the oil and natural gas subsector policy coordination and planning entity to collaborate with DOE as the SRMA and chair of the GCC. • Represent principal entry point for the government to collaborate with the oil and natural gas subsector for critical infrastructure security and resilience activities. • Serve as a strategic communication and coordination mechanism between owners, operators, suppliers, and, as appropriate, the government during emerging threats or response and recovery operations. • Participate in planning efforts related to the revision of the *National Infrastructure Protection Plan* and the development and revision of the energy sector-specific plan. • Review the annual submission to DHS on oil and natural gas subsector activities. • Understand and communicate requirements of the subsector for government support. • Provide input to the government on research and development efforts and requirements for the oil and natural gas subsector.
Electricity Information Sharing and Analysis Center	• Provide trusted communities and frameworks for critical infrastructure sectors to facilitate the sharing of timely, actionable, and reliable information for situational awareness. • Provide in-depth comprehensive sector threat and incident analysis and enable aggregation and anonymization of data. • Provide all-hazards threat warning and incident reporting to enhance member risk mitigation activities. • Participate in the planning, coordination, and conduct of energy sector exercises.
Energy Threat Analysis Center	• Work with the sector's information sharing and analysis centers and sector owners and operators to conduct advanced analysis of threats and incidents affecting the energy sector. • Enable shoulder-to-shoulder collaboration between the federal government and critical infrastructure owners and operators, including the fusing of information and sharing of analytic tools and capabilities. • Develop targeted guidance for the energy sector based on government-issued threat alerts for dissemination via the sector's information sharing and analysis centers. • Provide support for ESF #12 activities in the event of an incident affecting energy systems.
Federally funded research and development centers	• Leverage analytic tools and processes in support of risk management activities affecting the energy sector. • Support research and development activities aimed at enhancing the security and resilience of energy sector infrastructure.