REPORT TO THE CISA DIRECTOR

Building Resilience and Reducing Systemic Risk to Critical Infrastructure

December 5, 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.

In March 2023, the Subcommittee was tasked with providing 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?

In September 2023, the Subcommittee provided CISA with initial recommendations on the attributes for the architecture of a sector's operational collaboration model and the tactical elements that can produce an effective architecture and capabilities.

There are three key principles which should be reflected in the architecture of a sector's operational collaboration model.

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

2. Illumination of the Battlefield - Provides early insights or warning capability of adversary's intent/capability to set the direction that industry and government should take to address these risks. Drives a risk-informed intelligence collection and analysis apparatus that integrates the capabilities and accesses of private sector and government organizations.

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.

Findings

The following is a supplement to the September 2023 report that provides recommendations for:

1. Building an Operational Collaboration Framework.
2. Designing an Operational Collaboration Maturity Model.

Also included are model architectures for Operational Collaboration.

Build an Operational Collaboration Framework: There is no United States Government (USG) policy providing a standard or definition for operational collaboration or outlining its component parts. Standards and best practices need to be established for stakeholders to be aligned. Critically, operational collaboration is not a solitary thing, but rather the sum of component efforts. Decomposing the functions and capabilities that comprise operational collaboration requires focused public-private effort.

Different sectors have applied varying mechanisms to engage with the USG in the three principles outlined above, with varying emphasis on the current areas focus of efforts. For instance, within the Communications Sector, strategic or longer-term risks are addressed at the CEO or CTO level within the President's National Security Telecommunications Advisory Committee (NSTAC) and the NSA/CISA Enduring Security Framework venue. Risk mitigation and analysis efforts are generally coordinated through the Sector Coordinating Council in various Critical Infrastructure Partnership Advisory Council (CIPAC) venues such as the Information & Communications Technology Supply Chain Risk Management Task Force, which is closely aligned with the NRMC efforts and Joint Cyber Defense Collaborative. Finally, more tactical incident responses are primarily under the purview of the National Coordinating Center / Communications Information Sharing & Analysis Center, which works with Emergency Support Function 2, and cyber collaboration is manifested in the NSA Cyber Collaboration Center. This approach within the Communications Sector reflects the varying expert input required for these efforts while ensuring these efforts are aligned through the commonality of private sector company participation. This is not to suggest that this architecture is appropriate for all Sectors, but it does align the direction set by CEO-level direction with risk manager engagement and response level implementation.

In the Financial Services Sector, strategic or longer-term risks are addressed at the Financial Services Sector Coordinating Council (FSSCC), which promotes security and resilience of the sector by promoting best practices and the development of effective policies. In addition, the financial regulators work together along with Treasury through the Financial and Banking Information Infrastructure Committee (FBIIC) to coordinate with the FSSCC on critical infrastructure resilience issues, including efforts related to information sharing, best practices, and incident response. The Financial Services Information Sharing Analysis Center (FS-ISAC) shares specific information pertaining to cybersecurity and physical risks and distributes recommendations for protective measures and practices to institutions across the sector. The Analysis & Resilience Center for Systemic Risk (ARC), which partners with the US Treasury and Intelligence Community, supports risk mitigation by analyzing systemic risk issues and developing solution opportunities for the industry. Financial sector trade associations, in addition to their public policy roles, also play operational functions supporting the sector.

CISA, as National Coordinator should work with critical infrastructure and the NIST National Cybersecurity Center of Excellence (NCCoE) on a project with the goal of (1) defining Operational Collaboration for the USG, and (2) laying out a Maturity Model—a system that accurately measures the maturity of operational collaboration for each sector/subsector that takes into consideration the unique characteristics and needs of each.

Recommendations

CISA should create a framework that:

- Makes explicit and emphasizes the need to incentivize collaboration with increased transparency on the roles and responsibilities, capabilities, and authorities of the private and public sector partners involved.
- Is broad and flexible enough to include all 16 critical infrastructure sectors/subsectors. The sectors are organized differently and have unique priorities and diverse needs. A standard should take those differences into consideration.
- Aligns with similar standards used by the USG to coordinate responses to physical threats (i.e., FEMA's National Preparedness System and National Response Framework).

- Is based on a cybersecurity response to a disruption no matter the cause (e.g., the cybersecurity repercussions of a natural disaster, etc.).
- Encompasses steady state and incident response collaboration.
- Recognizes the differences between the ways different USG agencies collaborate with the private sector and clarifies the roles in those relationships.
- Outlines a mechanism for governance.
- Describes what successful collaboration looks like at the strategic, risk mitigation, and operational levels. Include the public policy efforts that levels.

CISA should create a maturity model that:

- Measures Cybersecurity Collaboration at risk, strategic, operational and public policy levels.
- Defines the planning horizons associated with each level of collaboration (e.g., risk is immediate/crises response, strategic is planning for likely incidents, operational is continual partnership, etc.).
- Includes steady state and incident response collaboration.
- Defines maturity as a repeatable process.
- Includes guidance on successful governance structures.

The CSAC continues to work and support CISA's development of new systems to identify and mitigate systemic risk to our nation's cyber and physical infrastructure. The heart of this work has been to operationalize the proposed collaboration between the private sector and the federal government. The recommendations provided, three sets to date, seek to illustrate this constructive collaboration. A change in legislation and authorities may be needed to overcome roadblocks for collaboration, information sharing and private-public sector partnerships.

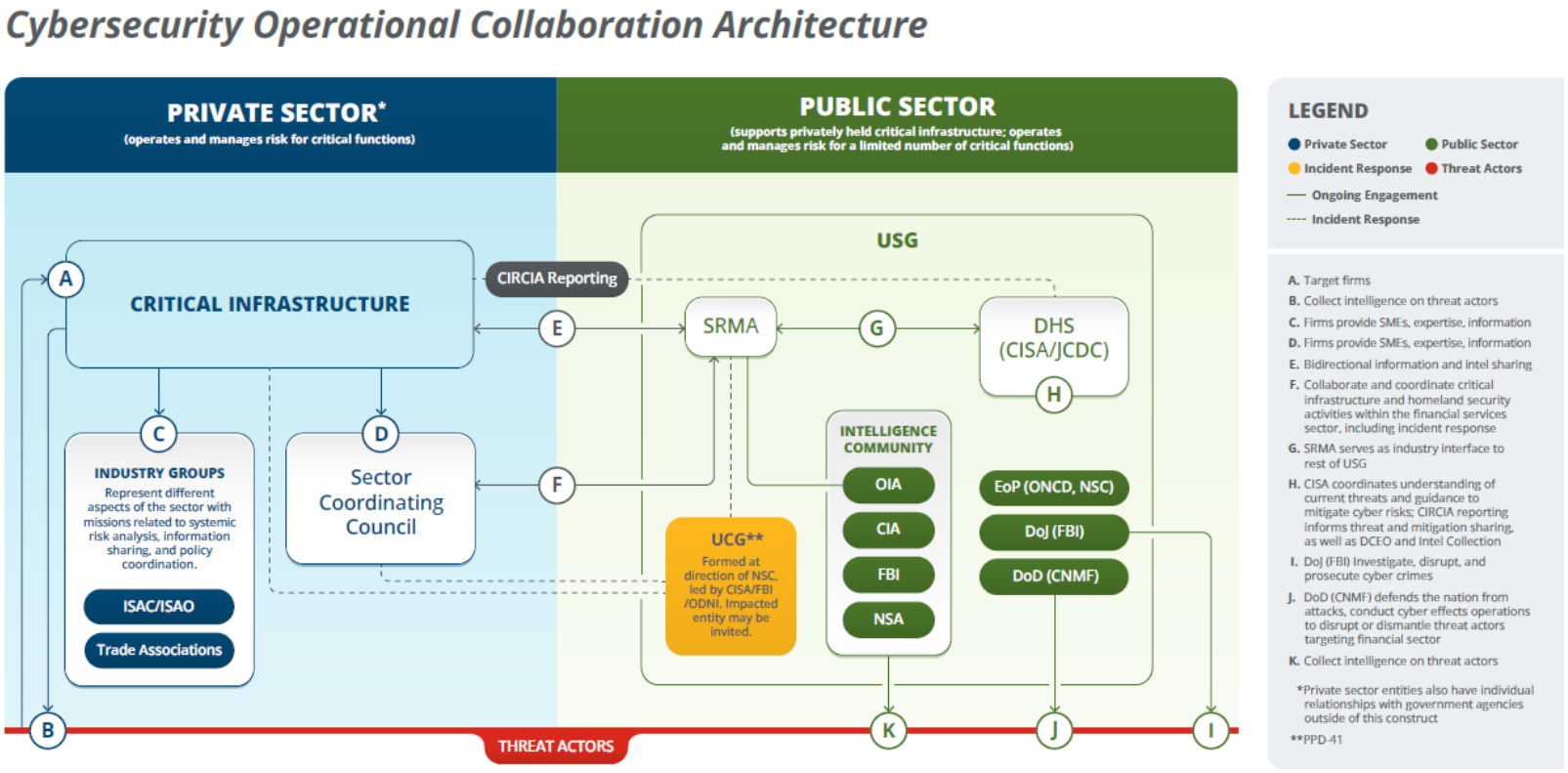
Appendix A:

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

Tom Fanning, SR 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: Sample Operational Collaboration Architectures

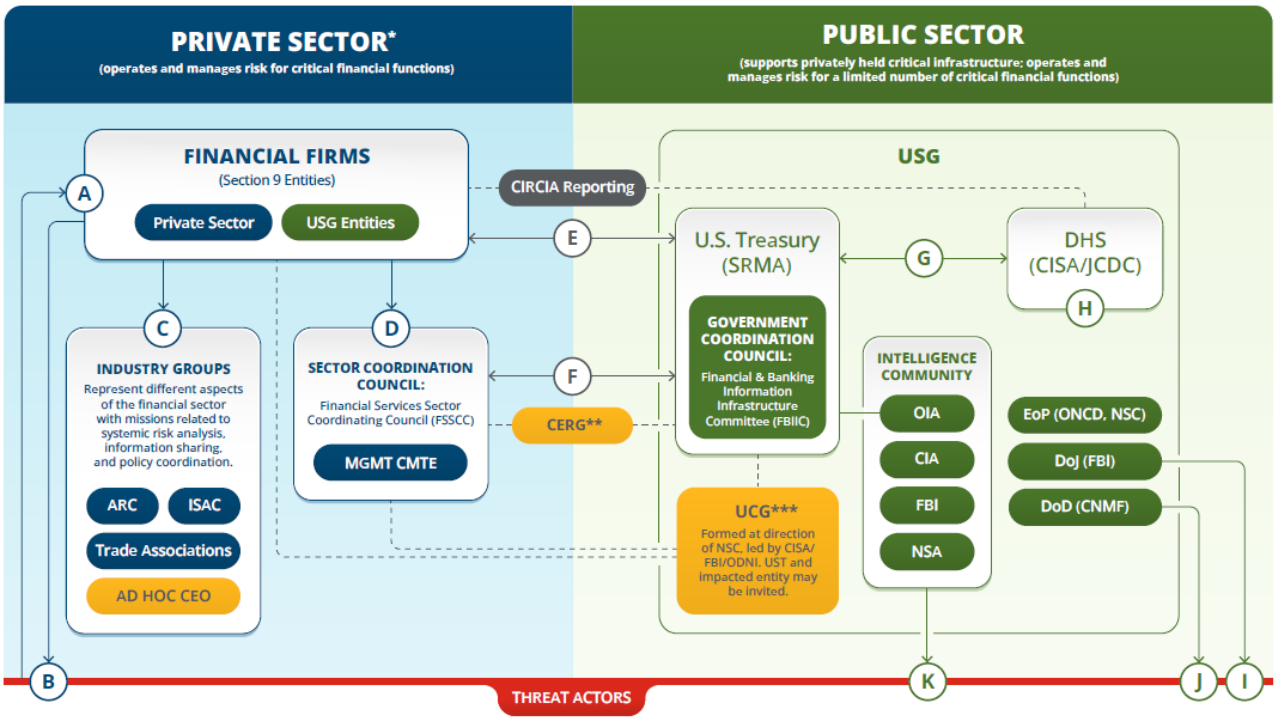
Generic Architecture



Financial Services Sector Architecture

Cybersecurity Operational Collaboration Architecture

Financial Services Sector



LEGEND

- Private Sector
- Public Sector
- Incident Response
- Threat Actors
- Ongoing Engagement
- Incident Response

A. Target all financial sector, especially Section 9 firms

B. Collect intelligence on threat actors

C. Firms provide SMEs, expertise, information

D. Firms provide SMEs, expertise, information

E. Bidirectional information and intel sharing

F. Collaborate and coordinate critical infrastructure and homeland security activities within the financial services sector, including incident response

G. SRMA serves as industry interface to rest of USG

H. CISA coordinates understanding of current threats and guidance to mitigate cyber risks; CIRCIA reporting informs threat and mitigation sharing, as well as DCEO and Intel Collection

I. DoJ (FBI) Investigate, disrupt, and prosecute cyber crimes

J. DoD (CNMF) defends the nation from attacks, conduct cyber effects operations to disrupt or dismantle threat actors targeting financial sector

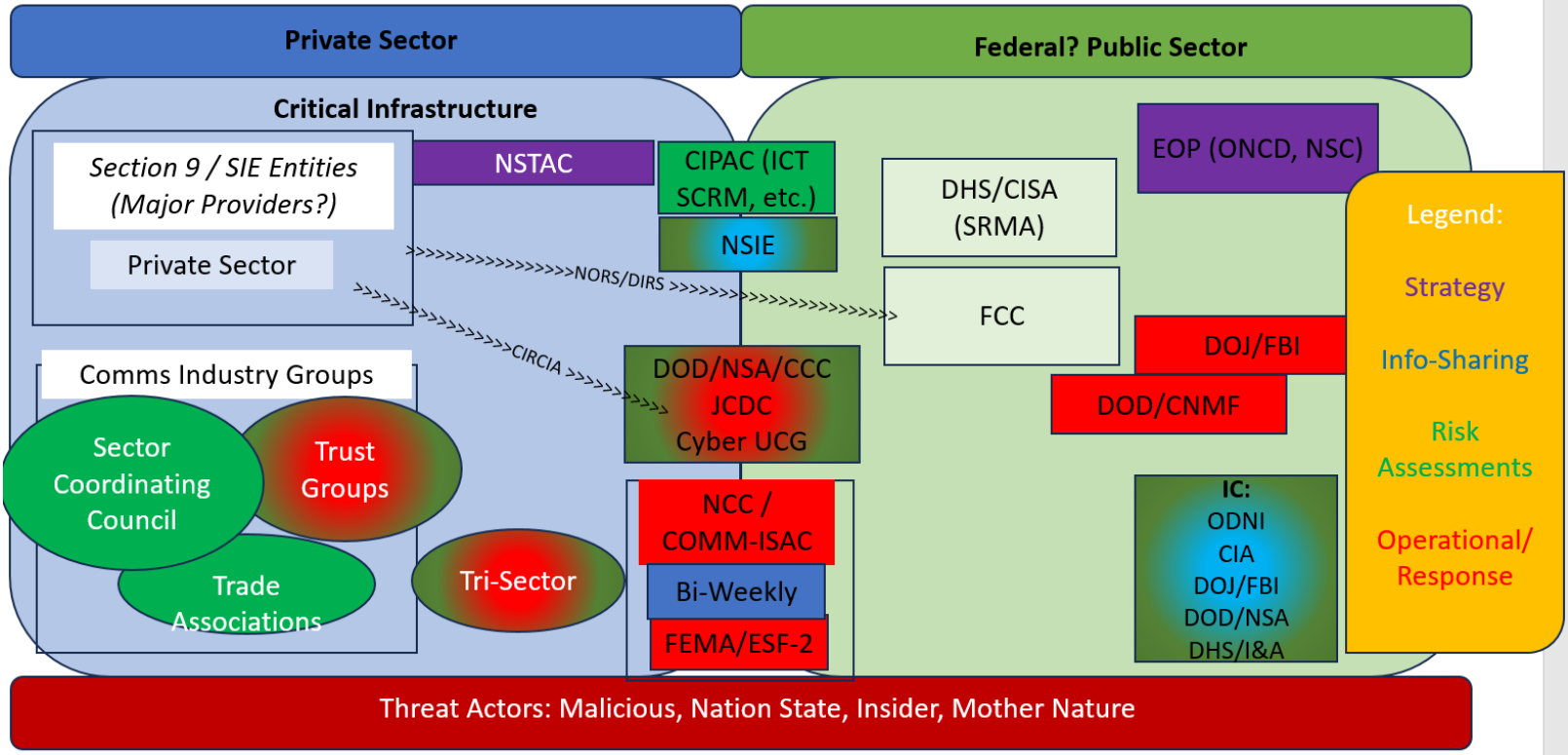
K. Collect intelligence on threat actors

*Private sector entities also have individual relationships with government agencies outside of this construct

**Core Executive Response Group (CERG) is made up of FS-ISAC, FBIIC, and FSSCC executive representatives and ensures information is shared as appropriate across the financial sector and sector response activities are coordinated during a significant event.

***PPD-41

Communications Sector Architecture



Electricity Subsector Architecture

Operational Collaboration Architecture