Roles and Responsibilities of the Sector Risk Management Agency for the Financial Services Sector

U.S. Department of the Treasury

October 2024

Table Of Contents

Overview

This report fulfills the requirement in the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) that:

> Within 180 days of the date of this memorandum, SRMAs, in coordination with the National Coordinator, shall develop plans to execute the required roles and responsibilities of each SRMA to ensure a continuity of effort and the coordination of policy and resourcing requirements.

In fulfillment of this requirement, this report outlines the enduring roles and responsibilities for the U.S. Department of the Treasury, as the designated Sector Risk Management Agency (SRMA) for the Financial Services Sector. The security and resilience of the Financial Services Sector depends on collaboration among a broad set of partners, including Financial Services Sector companies; sector trade associations; U.S. government agencies; financial regulators; state, local, tribal, and territorial governments; vendors; and other partners in the U.S. and internationally.

Treasury aims to ensure the United States maintains the world's most secure and resilient financial system by spearheading whole-of-nation efforts to increase the cybersecurity and resilience of the U.S. financial system. Treasury works collaboratively with its public and private sector partners to plan and execute the SRMA responsibilities directed in 6 U.S.C. § 665d. In terms of maturity, Treasury has long been an innovative SRMA that is at the forefront of public-private sector coordination and collaboration, leads risk management activities with the Financial Services Sector, and continuously develops new risk management solutions to address ever-evolving Financial Services Sector risks.

Roles

Treasury has clearly defined SRMA roles within the Department and relies on a host of other partners across the ecosystem to help Treasury provide specialized expertise to critical infrastructure owners and operators within the Financial Services Sector and support programs and associated activities of the sector. Treasury's SRMA function depends on collaboration and coordination across the Department and the federal government, with the Financial Services Sector regulatory agencies, the organizations representing the private sector firms that own and operate financial sector critical infrastructure, and the international community.

ACCOUNTABLE SENIOR OFFICIAL

Treasury designated the Senate-confirmed Assistant Secretary for Financial Institutions to serve as the Accountable Senior Official for the SRMA function for the Financial Services Sector. The Assistant Secretary for Financial Institutions is responsible and accountable for the implementation and performance of all of Treasury's SRMA roles and responsibilities.

DESIGNATED OFFICE AND STRUCTURE

The Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), reporting to the Treasury Assistant Secretary for Financial Institutions, leads the SRMA function within Treasury. OCCIP serves as the designated office to coordinate policy development to enhance the security and resiliency of the Financial Services Sector's critical infrastructure. OCCIP also provides expertise and support to the Financial Services Sector programs and associated activities. To fulfill this role, OCCIP works with the Department of Homeland Security as the National Coordinator and other relevant federal departments and agencies, collaborates with Financial Services Sector critical infrastructure owners and operators, and coordinates with Financial Services Sector regulatory agencies.

OCCIP reports to the Assistant Secretary for Financial Institutions within Treasury's Office of Domestic Finance. The Office of Domestic Finance, led by a Senate-confirmed Under Secretary, advises and assists the Secretary of the Treasury with areas of domestic finance, banking, and other related matters. Domestic Finance develops policies and guidance for Treasury activities related to financial institutions, federal debt finance, financial regulation, and capital markets.

The Deputy Assistant Secretary for Cybersecurity and Critical Infrastructure Protection leads OCCIP, which consists of two directorships: (1) Sector Cyber Intelligence, Risk Analysis, and Resilience and (2) Domestic and International Cyber Policy. The directorships encompass four teams with varied capabilities to enhance operational functions in support of the SRMA role. SRMA workstreams typically apply cross-team integration within OCCIP to leverage specialized staff expertise. Figure 1 illustrates the organization chart. OCCIP is supported by a staff of approximately 30 full-time FTEs from grades GS-11 to the Senior Executive level.

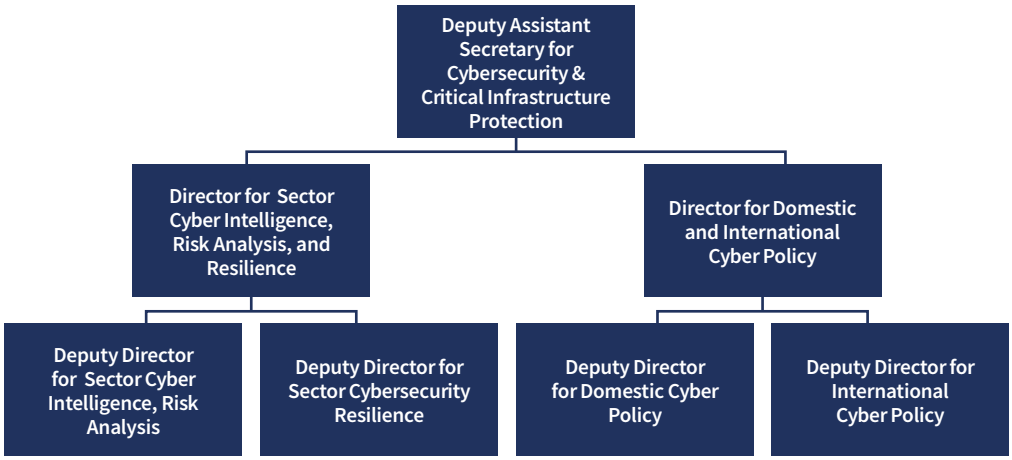

Figure 1. The Office of Cybersecurity and Critical Infrastructure Protection Structure

DEPARTMENT INTEGRATION

As a whole-of-Department effort, Treasury leverages expertise from selected offices and bureaus to enable the SRMA responsibilities coordinated by OCCIP:

- Bureau of the Fiscal Service
- Financial Crimes Enforcement Network
- Financial Stability Oversight Council
- Office of the Chief Information Officer
- Office of the Comptroller of the Currency
- Office of Financial Research
- Office of Foreign Assets Control
- Office of Intelligence and Analysis
- Office of Terrorist Financing and Financial Crimes

PARTNERSHIPS

The Financial Services Sector operates with enduring relationships to government entities across the interagency and independent regulators. The close ties derive from multiple longstanding structural factors: (1) Treasury owns and operates certain critical infrastructure as part of the sector; (2) multiple activities within the sector have been designated as National Critical Functions; (3) independent regulators – many of which are government institutions at the national and state levels – regulate traditional Financial Services Sector firms; and, (4) government entities provide support to the Financial Services Sector including intelligence, law enforcement, standards, and policy development.

FINANCIAL SERVICES GOVERNMENT COORDINATING COUNCIL

Financial Services Sector independent regulators formally interact on critical infrastructure and operational resiliency through the Financial and Banking Information Infrastructure Committee (FBIIC), designated as the Government Coordinating Council for the Financial Services Sector. The Treasury Assistant Secretary for Financial Institutions chairs the FBIIC. Treasury coordinates incident, policy, information, and intelligence sharing with appropriate FBIIC members. FBIIC provides expertise to Treasury and interagency policy workstreams regarding Financial Services Sector operations, risk, vulnerabilities, and incidents. FBIIC participates as a member in the Department of Homeland Security Critical Infrastructure Partnership Advisory Council.

U.S. GOVERNMENT INTERAGENCY

Treasury, as the SRMA, fosters robust multilateral policy coordination and information sharing across Executive Branch departments and agencies. In accordance with Presidential Policy Directive 41, for coordinating responses to significant cyber incidents, Treasury relies upon the Department of Justice for threat response activities, the Department of Homeland Security for asset response activities, and the Office of the Director of National Intelligence for intelligence support and related activities. Treasury participates in the established national operational coordination mechanisms, including the Cyber Response Group and, when formed, the Cyber Unified Coordination Group.

Treasury, as Chair of the Committee on Foreign Investment in the United States, works with the Committee's members to address national security risks related to critical infrastructure, among other things, as may arise in the context of certain foreign investments into U.S. businesses and certain real estate transactions by foreign persons to determine the effect of such transactions on the national security of the United States.

Historically, Treasury has leveraged co-located detailees from regulators, federal law enforcement, and Intelligence Community agencies to enhance its SRMA execution. In addition, Treasury has co-located liaisons and detailees at the Cybersecurity & Infrastructure Security Agency (CISA), federal law enforcement, and Intelligence Community agencies. Going forward, Treasury envisions using the Treasury Cyber Collaboration Suite (T-Suite), led by Treasury's Office of Intelligence and Analysis, to host co-located Intelligence Community, interagency, and cleared industry staff. Treasury uses Memoranda of Understanding to govern these staffing relationships and formal collaboration between stakeholders.

INTERNATIONAL GOVERNMENT PARTNERS

Treasury fosters relationships with counterpart organizations in international governments to enhance resilience and in support of the Financial Services Sector's integration into the larger global economy. Regular, ad hoc, and project-specific collaboration with these partners ensures that Treasury's SRMA efforts are informed by international best practices in risk management. Additionally, Treasury co-chairs the Group of Seven (G7) Cyber Expert Group (CEG) and coordinates cybersecurity policy and strategy across the G7 jurisdictions.

FINANCIAL SERVICES SECTOR COORDINATING COUNCIL

The Financial Services Sector Coordinating Council (FSSCC) advocates for alignment of government policies and activities with the needs of the entire sector, sector critical functions, and individual critical infrastructure firms. FSSCC routinely interacts with the government through leadership meetings, committees, and events (i.e., FSSCC events and joint FSSCC/FBIIC events). The FSSCC provides input to the interagency to design effective government programs, services, and information sharing related to Financial Services Sector security and resiliency. FSSCC represents the private sector in CISA and interagency cross-sector deliberative bodies.

FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER

The Financial Services Information Sharing and Analysis Center (FS-ISAC) provides a real-time information-sharing network that amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defense. Treasury and interagency partners use FS-ISAC as the primary mechanism to rapidly share information across the sector. Treasury and FS-ISAC collaborate to share information issues that impact the sector to identify, assess, and reduce risk. FS-ISAC works with other sectors' ISACs to enable cross-sector collaboration and to reduce risk incurred by Financial Services Sector dependencies on other sectors. Treasury maintains a current membership in FS-ISAC.

FINANCIAL SECTOR CORE EXECUTIVE RESPONSE GROUP

The Financial Sector Core Executive Response Group (CERG) is an all-hazards public-private crisis coordination body consisting of a small group of trusted parties from several key Financial Services Sector entities and financial regulators. The CERG develops an understanding of the scope and scale of an incident or imminent threat and assesses the potential systemic risks. The CERG's primary goals are to 1) enhance the sector's ability to assess sector risk through a shared understanding of the incident or threat, 2) identify sector-level policy priorities, and 3) collaborate on media response during disruptive events. The CERG does not engage in response activities for incidents or prescribe response actions for its members or others.

TRADE ASSOCIATIONS

Financial Services Sector trade associations have deep expertise in their respective areas (i.e., banking, finance, and investment) within the sector. Using this deep expertise, in coordination with the FSSCC, Treasury works with the trade associations on policy issues. The trade associations play a role in managing extreme all-hazards events to ensure the integrity and continued operation of the financial markets. As appropriate, Treasury relies on trade associations to facilitate targeted outreach to support events and develop exercises.

Responsibilities

Treasury collaborates closely with Financial Services Sector companies, industry groups, and government partners to fulfill Treasury's statutory SRMA responsibilities directed in 6 U.S.C. § 665d. Treasury leverages this Financial Services Sector expertise to support sector risk management, assess sector risks, perform sector coordination, facilitate the sharing of information on physical security and cybersecurity threats, support incident management, and contribute to emergency preparedness efforts.

SUPPORT SECTOR RISK MANAGEMENT

Treasury supports sector risk management through various enduring programs and joint workstreams with both the FBIIC and FSSCC, as they relate to risks to critical infrastructure owners and operators within the Financial Services Sector by identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets. The risk-specific workstreams may change over time as new priority risks emerge and will be identified in subsequent Financial Services Sector Risk Management Plans. Treasury recommends security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets to the Financial Services Sector through these programs and workstreams.

Treasury developed and will continue to use the Cloud Executive Steering Group (CESG) model to manage significant risk-specific workstreams. The CESG is a public-private partnership chaired by agency heads and sector chief executive officers in the FBIIC and FSSCC that oversee related risk mitigation efforts. This model bolsters regulatory and private sector cooperation and has been effective in addressing cybersecurity and

resiliency issues. Separately, Treasury leverages interagency partners, especially through the Joint Cyber Defense Collaborative, to collaborate on cross-sector initiatives to identify and mitigate risks that could impact Financial Services Sector operations.

ASSESS SECTOR RISK

Treasury runs a risk management program designed to identify, assess, and recommend prioritization of operational risks to Financial Services Sector critical infrastructure. The risk management program provides a structured, data-driven approach that enables Treasury to: (1) establish a common operational risk baseline for the Financial Services Sector, (2) advise Treasury leadership, the FBIIC, and other stakeholders on operational risks to the Financial Services Sector, and (3) inform and prioritize cybersecurity and resilience policies, programs, and initiatives.

Treasury supports national risk assessment efforts led by the White House and those led by CISA's National Risk Management Center, to include participating in interagency meetings, data calls, report writing, and any other collective effort as required. In this capacity, Treasury serves as an advocate for the Financial Services Sector and provides financial services subject matter expertise to national-level risk assessment efforts. Treasury also supports risk analysis conducted by the Financial Services Sector, primarily through the Analysis and Resilience Center for Systemic Risk (ARC). The ARC is a coalition of financial services firms that own and operate the nation's most critical financial infrastructure that work together to identify, prioritize, and mitigate systemic risk to that infrastructure. Treasury co-chairs the ARC's Public Sector Risk Committee.

Treasury will coordinate with the National Coordinator and public partners to provide input for the list of Systemically Important Entities (SIE). The SIE list shall inform prioritization of federal activities, including the provision of risk mitigation information and other operational resources to non-federal entities.

SECTOR COORDINATION

Treasury serves as the day-to-day federal interface for the prioritization and coordination of Financial Services Sector SRMA activities and responsibilities. In this capacity, Treasury chairs the FBIIC and is the focal point for all government partners regarding the Financial Services Sector. Through the G7 CEG, Treasury works with international partners to support sector risk management and produce informational resources to support critical infrastructure owners and operators in their efforts in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems.

On the private sector side, Treasury formally relies on the FSSCC to provide policy input, positions, and prioritization on behalf of Financial Services Sector firms and trade associations. In some instances, FSSCC furthers Treasury's SRMA role by coordinating directly with FBIIC members. Treasury also persistently engages with FS-ISAC for day-to-day operational updates and analysis on emerging technology issues (i.e., cloud, artificial intelligence, and quantum) that Treasury uses for coordination with the private sector, interagency, and independent regulators.

INFORMATION SHARING

With unclassified and classified briefing programs, original production, and downgraded intelligence, Treasury facilitates and disseminates bi-directional information sharing of actionable, timely, and relevant physical security and cybersecurity threats with the Financial Services Sector. To support the sharing of classified information, Treasury identifies and nominates Financial Services Sector individuals for security clearances in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, and facilitates classified information sharing via the T-Suite.

Treasury supports victim notification efforts led by the Federal Bureau of Investigation (FBI) and CISA to Financial Services Sector entities. In addition, when necessary, Treasury may facilitate outreach and provide mitigation guidance to individual firms when an identified security incident is present. Treasury also provides input regarding priority threats, vulnerabilities, and mitigations about which CISA and other interagency partners should prioritize its analysis, expertise, coordination, and product releases.

SUPPORT INCIDENT MANAGEMENT

Treasury's incident response program is responsible for coordinating public-private sector activities during a major incident affecting the Financial Services Sector. Treasury primarily uses the FBIIC Incident Response Protocol that is aligned with the National Cyber Incident Response Plan and designed for FBIIC members to coordinate unity of effort and unity of message. This coordination mechanism facilitates unified engagement with identified Financial Services Sector and U.S. government stakeholders and across other critical infrastructure sectors by connecting the FBIIC to efforts underway across the critical infrastructure sectors, law enforcement, and the National Security Council, including through the Cyber Response Group and, when formed, the Cyber Unified Coordination Group.

Further, Treasury formally participates in the CERG to coordinate incident response activities with Financial Services Sector leadership during significant security incidents and other crises. As a critical infrastructure owner and operator, Treasury coordinates incident activities with internal Department stakeholders to ensure situational awareness and expectations between external and internal stakeholders are aligned. Treasury also maintains a Cyber Incident Communications Playbook containing communications protocols that aides Treasury's work with its interagency and private sector partners to manage a coherent public communications response during incidents.

CONTRIBUTE TO EMERGENCY PREPAREDNESS

Treasury contributes to emergency preparedness through the development of planning documents for coordinated action during an emergency. This is accomplished primarily through the development of response protocols and playbooks used for the Support Incident Management activities. Treasury also supports national-level emergency preparedness efforts by serving as the Financial Services Sector government coordination point for Emergency Support Function 2 (ESF2) and Emergency Support Function 14 (ESF14). ESF2 supports the restoration of communications infrastructure, coordinates

communications support to response efforts, facilitates the delivery of information to emergency management decision makers, and assists in the stabilization and reestablishment of systems and applications during incidents. ESF14 supports the coordination of cross-sector operations, including stabilization of key supply chains and community lifelines, among infrastructure owner and operators, businesses, and their government partners. ESF2 and ESF14 provide an avenue to the U.S. government for information sharing and coordination, including requests for assistance in situations where private sector organizations do not have a designated ESF, sector partner, or other mechanism for coordination.

Further, Treasury contributes to emergency preparedness through its Hamilton Exercise Program, which provides the Department, the interagency, and the Financial Services Sector with tailored exercises designed to prepare organizations for responding to emergencies and improve overall sector resilience. Treasury provides support to exercises run by other organizations and entities. These include but are not limited to national-level exercises, international exercises, and sector-led exercises. Treasury works directly with other entities as part of the planning team on shaping the purpose, objectives, and design of the exercise, and during execution as exercise participants.

U.S. Department of the Treasury

TREASURY.gov