

Financial Services Sector Government Coordinating Council Charter

Article I – Background and Official Designation

National Security Memorandum 22/NSM-22 Critical Infrastructure Security and Resilience designates the U.S. Department of the Treasury as the Sector Risk Management Agency (SRMA) for the Financial Services Sector. The SRMA function spans a number of responsibilities that include serving as a coordination hub for collaboration among public and private sector entities on sector-specific issues pertaining to cybersecurity, infrastructure security, and resilience; coordinating and prioritizing sector-wide activities, including those related to education, training, information sharing, and outreach; providing incident management support in accordance with the appropriate policies and directives; facilitating access to resources and services in support of risk management efforts across the sector; and leading sector-wide strategic planning activities.

SRMA engagement with federal departments and agencies, and state, local, tribal, and territorial (SLTT) entities is conducted through the partnership structure established in the National Infrastructure Protection Plan (NIPP) as the “Financial Services Sector Government Coordinating Council,” hereinafter referred to as “FSGCC” or “council.” The FSGCC is commonly referred to as the Financial and Banking Information Infrastructure Committee (FBIIIC).

The FSGCC supports the sector’s cybersecurity and infrastructure security mission in accordance with *National Security Memorandum 22/NSM-22 Critical Infrastructure Security and Resilience*, *Presidential Policy Directive/PPD-41 United States Cyber Incident Coordination*, and other applicable critical infrastructure policies, guidelines, and directives.

Article II – Mission and Purpose

The mission and purpose of the FSGCC is to provide effective interagency, intergovernmental, and cross-jurisdictional coordination of activities, strategies, and policy that are relevant to the cybersecurity, infrastructure security, and resilience of the Financial Services Sector.

The FSGCC acts as the counterpart and partner to the private industry-led Financial Services Sector Coordinating Council (FSSCC) to plan, prioritize, coordinate, implement and execute sufficient and necessary sector-wide cybersecurity, infrastructure security, and resilience efforts.

Article III – Objectives and Scope of Activity

The FSGCC supports the mission through the following objectives:

- Facilitate coordination among member agencies on issues pertaining to the cybersecurity, infrastructure security, and resilience of the sector.
- Integrate relevant cybersecurity, infrastructure security, and resilience-enhancing initiatives among member agencies.
- Foster effective dialogue and information sharing among owners, operators, and regulators of Financial Services Sector infrastructure, and other sector partners.
- Promote collaboration with other critical infrastructure sectors.
- Develop workstreams that advance the FSGCC member agencies' collective understanding of financial sector critical functions and operations and the resilience thereof.
- Partner with relevant departments and agencies to improve intelligence support on cyber and other threats to the Financial Services Sector.
- Identify and remove impediments to knowledge sharing regarding risks, threats, vulnerabilities, best practices, and resilience.

The scope of FSGCC activities includes, but is not limited to:

- Work together to promote continuous improvement of cybersecurity, infrastructure security, and resilience-enhancing efforts within the sector as national and sector goals and priorities are identified.
- Promote adoption and implementation of effective risk management processes, best practices, and use of innovative methods across the sector.
- Identify and support the information-sharing capabilities and mechanisms that are most appropriate for government and industry entities.
- Coordinate with and support the efforts of sector partners to plan, implement, and execute the Nation's homeland security mission.
- Report on the progress made for addressing goals and objectives and applicable national priorities.
- Acknowledge and respond to concerns of the sector, from both public and private-sector entities, and work in coordination with the FSSCC to address and resolve those concerns when possible.
- Collaborate with the FSSCC to foster a coordinated sector-wide approach to physical and/or cyber incidents affecting the sector during periods of heightened awareness, in accordance with corresponding authorities, policies, and directives applicable to each agency.

Article IV – Membership and Member Representatives

Membership

The SRMA is responsible for identifying and organizing a representational FSGCC to include other federal departments and agencies and, as needed, SLTT government agencies with responsibilities relevant to the cybersecurity, infrastructure security, and resilience posture of the sector. The composition of the FSGCC shall be consistent with the operational landscape of the sector. Membership resides with the department/agency rather than the individual representatives.

The FSGCC consists of 18 member organizations from across the financial regulatory community, both federal and state.

- | | |
|---|--|
| • Department of the Treasury, FSGCC Chair | • Board of Governors of the Federal Reserve System |
| • American Council of State Savings Supervisors | • National Association of Insurance Commissioners |
| • Commodity Futures Trading Commission | • National Association of State Credit Union Supervisors |
| • Conference of State Bank Supervisors | • National Credit Union Administration |
| • Consumer Financial Protection Bureau | • North American Securities Administrators Association |
| • Farm Credit Administration | • Office of the Comptroller of the Currency |
| • Federal Deposit Insurance Corporation | • Securities and Exchange Commission |
| • Federal Housing Finance Agency | • Securities Investor Protection Corporation |
| • Federal Reserve Bank of Chicago | |
| • Federal Reserve Bank of New York | |

Voting Members

Membership resides with the participating agency member, which selects its primary and alternate representative(s) at the appropriate decision-making level to achieve the objectives of the FSGCC. The SRMA management staff maintains a record of the designated primary and alternate representative(s) for each voting member.

Non-voting

The FSGCC may include representatives or designated liaisons from other sector and cross-sector GCCs, other government agencies, or international governmental entities to participate in a non-voting capacity. Non-voting members do not serve in council or working group leadership roles as required under the Critical Infrastructure Partnership Advisory Council (CIPAC) Charter and may be withdrawn at any time at the discretion of the SRMA. The SRMA management staff maintains a record of the designated representative(s) for each non-voting member.

Subject Matter Experts

The FSGCC reserves the right to invite subject matter experts to contribute expertise as needed in support of specific meetings or activities. A subject matter expert's individual expertise or opinion may be used to provide technical or industry-specific information for the purposes of informing the recommendations made by the council. Subject matter experts are non-voting participants of the FSGCC and do not serve in council or working group leadership roles as required under the CIPAC Charter.

Article V – Officers and Governance

Officers

The FSGCC is chaired by the U.S. Department of the Treasury as the SRMA for the Financial Services Sector. The Deputy Assistant Secretary, Cybersecurity and Critical Infrastructure Protection, serves as the Chair.

The Chair may designate SRMA management designee(s) to act on his/her/their behalf, oversee the corresponding SRMA management responsibilities, and direct the SRMA management staff in the execution of those responsibilities.

It is the responsibility of the Chair to:

- Maintain council membership and representation, facilitate decision-making processes, work in consultation with council membership, and provide cross-sector coordination with SLTT governments.
- Coordinate development and distribution of work products.
- Coordinate development and submittal of responses to requests for information directed to the FSGCC.
- Initiate and facilitate FSGCC meetings, to include:
 - Agenda development.
 - Issues and initiative monitoring, and completion of action items.
 - Administrative and logistical meeting support.
 - Preparation and distribution of meeting minutes.
 - Notification and communications.
- Determine the need for and recommend establishment of FSGCC working groups, subject to FBIIC membership concurrence.
- Manage council records.
- Maintain council Charter and other council and/or working group governance documents.

The Chair initiates the coordination and facilitation of joint FSGCC and FSSCC meetings with FSSCC leadership – including meetings conducted under the auspices of CIPAC – thereby ensuring compliance with the CIPAC Charter.

Governance

Council members make decisions through a consultative process and consensus.

The Chair recognizes that each member represents a government entity with inherent legal authority to operate. When there is dissension, the Chair may move forward as a standalone agency, without invoking the names of the other FSGCC government entities. Members will strive to meet timelines and deliverables on a best-efforts basis.

Article VI – Meetings

The FSGCC will meet at least six times a year in the Washington, DC area and/or at an alternative location determined by FSGCC members. Additional meetings are scheduled as needed. Meetings are held in-person, virtually, and/or telephonically and follow Robert’s Rules of Order.

Article VII – Working Groups

Working groups and affiliated sub-working groups are established when substantial investigation, research, or other tasks are required that cannot be practicably achieved at regular council meetings. All working groups are meant to advise council members on various issues and processes. Through their primary or alternate representatives, each member agency may designate individuals to serve on working groups or serve as working group leads.

The council establishes working groups that:

- Consist of personnel selected by the Chair or council based on the issue under study and expertise.
- Have a specific and clearly defined mission and scope, time limit, and deliverable(s).
- Select a working group chair charged with leading the working group in achieving its objective, on time and within scope to the extent possible.
- Are subordinate to the council and report activities and recommendations to the council.

When the FSGCC and FSSCC form joint working groups, the FSGCC working group chair will work in close coordination with the corresponding FSSCC working group chair. Joint FSGCC and FSSCC working groups may conduct meetings/activities under the auspices of CIPAC when consensus to form recommendations is needed and the group is established in compliance with CIPAC Designated Federal Officer (DFO) guidelines.

Article VIII– CIPAC Membership and Compliance

CIPAC Compliance

CIPAC facilitates interactions across federal and SLTT government levels and representatives from the community of critical infrastructure owners and operators to conduct deliberations that form consensus positions to present to the federal government related to cybersecurity and infrastructure security matters.

Meetings consisting solely of FSGCC members do not constitute CIPAC meetings. To conduct or participate in CIPAC activities, the FSGCC will maintain its Charter, a representational membership and comply with the requirements defined in the CIPAC Charter and guidance issued by the DFO.

CIPAC Member and CIPAC Member Representative

Members of the FSGCC are automatically members of CIPAC upon notification by the Chair to the CIPAC Executive Secretariat/DFO for posting to the publicly accessible CIPAC Financial Services Sector: Council Charters and Membership [website](#). Membership is managed and maintained by the Chair providing a roster listing each member organization to the CIPAC Executive Secretariat/DFO at CIPAC@cisa.dhs.gov annually or as changes occur.

Article IX – Communications

The SRMA management staff are to maintain the appropriate communication mechanisms for sharing information among FSGCC membership and, when applicable, with the FSSCC and other relevant sector partners and stakeholders, in accordance with all applicable information sharing agreements, laws, and regulations.

Article X – Recordkeeping

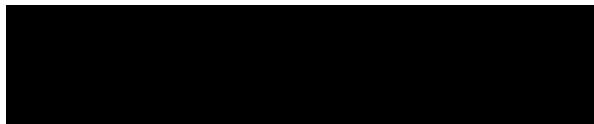
The procedures for the handling, storage, and disposition of FSGCC records and other documentation are the responsibility of the SRMA management staff in accordance with DHS/CISA and Federal Records Act policies.

Article XI – Amendments

The Chair on behalf of the FSGCC may at any time initiate amendments to this Charter. The amended Charter will be coordinated with FSGCC members and submitted to the CIPAC DFO in a timely manner for posting on the public CIPAC website.

Article XII – Approval and Duration

This Charter is approved as attested to by the following signature authority and will be in effect for a period not to exceed five years.



Todd Conklin
Deputy Assistant Secretary
Cybersecurity and Critical Infrastructure Protection
U.S. Department of the Treasury

11/12/2024

Date