Information Technology Sector Government Coordinating Council Charter

Article I – Background and Official Designation

Presidential Policy Directive/PPD-21 Critical Infrastructure Security and Resilience designates the U.S. Department of Homeland Security (DHS) as the Sector Specific Agency (SSA) for the Information Technology (IT) Sector. The SSA 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 awareness, education, training, information-sharing, and outreach; providing incident management support in accordance with 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.

SSA 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 "Information Technology Government Coordinating Council," hereinafter referred to as "GCC" or "council".

The GCC supports the sector's cybersecurity and infrastructure security mission in accordance with *Presidential Policy Directive/PPD-21 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 GCC 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 Information Technology Sector.

The GCC acts as the counterpart and partner to the private industry-led Information Technology Sector Coordinating Council (SCC) 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 GCC supports the mission through the following objectives:

- Increase the level of coordination among member agencies on relevant issues pertaining to the cybersecurity, infrastructure security, and resilience of the sector.
- Improve integration of relevant cybersecurity, infrastructure security, and resilience-enhancing initiatives among member agencies.
- Foster effective dialog and information sharing among owners, regulators, non-government owners, and other sector partners.
- Promote collaboration with other critical infrastructure sectors.
- Identify, prioritize and coordinate the IT Sector's critical infrastructure security and resilience (CISR) activities with a range of public and private sector stakeholders.
- Identify the IT Sector's needs or gaps in current IT-related risk management activities plans, programs, policies, procedures, and strategies, as well as measure their effectiveness.
- Promote awareness of current IT Sector activities within the sector and across the other critical infrastructure sectors.

- Invite Federal and SLTT representatives to share their experiences, ideas, best practices, and innovative approaches related to IT Sector CISR.

The scope of GCC 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 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 SCC to address and resolve those concerns when possible.
- Collaborate with the SCC to foster a coordinated sector-wide approach to physical or cyber incidents affecting the sector or during periods of heightened awareness, in accordance to the corresponding authorities, policies, and directives applicable to each agency.

Article IV – Membership and Member Representatives

Membership

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

GCC member roles and responsibilities include:

- Partner with the GCC Chair, CISA Stakeholder Engagement Division and other GCC members to develop strategic communications for the IT Sector's CISR planning and coordination, and facilitate the discussion and resolution of CISR-related issues;
- Enhance the foundation for protective programs with sector partners;
- Lend subject matter expertise to the GCC to identify and prioritize sector challenges and risks;
- Coordinate with, and support select efforts of, the SCC to plan, implement, and execute the nation's Information Technology CISR mission;
- Participate in planning, developing, implementing, updating, and revising the Information Technology Sector-Specific Plan and Sector Annual Reporting; and
- Collaborate with private and public sector partners to share CISR-related information (e.g., experiences, best practices, lessons learned, etc.) within the Information Technology Sector, as appropriate.

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 GCC. The SSA management staff maintains a record of the designated primary and alternate representative(s) for each voting member.

Non-voting

The GCC 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 membership may be withdrawn at any time at the discretion of the SSA. The SSA management staff maintains a record of the designated representative(s) for each non-voting member.

Subject Matter Experts

The GCC 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 GCC and do not serve in council or working group leadership roles as required under the CIPAC charter.

Article V – Officers and Governance

Officers

The GCC is chaired by the Cybersecurity and Infrastructure Security Agency (CISA) as the SSA for the Information Technology Sector. As the SSA Principal, the Director for CISA serves as the chairperson for the GCC.

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

It is the responsibility of the chairperson/SSA management designee to:

- Maintain council membership and representation, facilitate decision-making processes, work in consultation with council membership, and provide cross-sector coordination with state, local, tribal and territorial (SLTT) governments.
- Coordinate development and distribution of work products.
- Coordinate development and submittal of responses to requests for information directed to the GCC;
- Initiate and facilitate GCC meetings, to include:
    - Develop agendas;
    - Monitor issues and initiatives, and completion of action items;
    - Provide administrative and logistical meeting support;
    - Prepare and distribute meeting minutes; and
    - Handle notifications and other communications.
- Determine the need for GCC working groups.
- Manage council records.
- Maintain council charter and other council and working group governance documents.

The chairperson/SSA management designee initiates the coordination and facilitation of joint GCC and SCC meetings with SCC leadership—including meetings conducted under the auspices of CIPAC—ensuring compliance with the CIPAC Charter.

Governance

Council members make decisions through a consultative process and consensus by simple majority of members present unless otherwise determined by the chairperson/SSA management designee. Member organizations have one vote regardless of the number of representatives present.

The GCC recognizes that each member represents a government entity with inherent legal authority to operate that may cause a representative to abstain from voting on certain matters. When there is

dissension, the chairperson/SSA management designee may move forward, and act to fulfill the obligations of the council. Members will strive to meet timelines and deliverables even when there is less than full agreement or participation.

Article VI – Meetings

The GCC will meet at least two times a year and as often as quarterly, in the Washington, DC, area or at an alternative location determined by GCC members. Additional meetings are scheduled as needed. Meetings are held in person 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 chairperson/SSA management designee or council based on the issue under study, scope and expertise.
- Have a specific and clearly defined mission and scope, time limit and deliverable(s).
- Select a working group chair charged with ensuring that the working group achieves its objective and stays on time within scope.
- Are subordinate to the council and reports activities and recommendations to the council.

When the Information Technology GCC and SCC form joint working groups, the GCC working group chairperson will work in close coordination with the corresponding SCC working group chairperson. Joint GCC and SCC 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 between government representatives at the federal, state, local, tribal and territorial 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 members of the GCC do not constitute meetings of the CIPAC. To conduct or participate in CIPAC activities, the GCC will maintain its charter and a representational membership and will comply with the requirements defined in the CIPAC charter and guidance issued by the CIPAC Designated Federal Officer (DFO).

CIPAC Member and CIPAC Member Representative

Members of the GCC are automatically members of CIPAC upon notification to the CIPAC Executive Secretariat/DFO for posting to the publicly accessible CIPAC website. Membership is managed and maintained by the chairperson/SSA management designee staff providing a roster with each representative's name, title, organization/component and contact information to the CIPAC Executive Secretariat/DFO at CIPAC@cisa.dhs.gov annually or as changes occur.

Article IX – Communications

The SSA management staff maintain the appropriate communication mechanisms for sharing information among GCC membership and, when applicable, the SCC and other relevant sector partners and stakeholders, in accordance with all applicable information-sharing laws and regulations.

Article X – Recordkeeping

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

Article XI – Amendments

The chairperson/SSA designee on behalf of the GCC may at any time initiate amendments to this charter. The amended charter will be 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.

Date **11/16/2020**

Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security