Information Technology Government Coordinating Council Charter

1. **Official Designation**
   The official designation of this Council is the "Information Technology Government Coordinating Council," hereinafter referred to as the "IT GCC." The IT GCC is a voluntary, advisory committee that is not appointed any decision-making authority.

2. **Authorities and Background**
   The IT GCC operates under the auspices of two primary authorities: (1) Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*; and (2) the National Infrastructure Protection Plan (NIPP). In accordance with PPD-21, the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C) coordinates the Nation's cyber and communications engagement initiatives with relevant Federal departments and agencies (D/A) and collaborates with critical infrastructure owners and operators; independent regulatory agencies; and State, Local, Tribal, and Territorial (SLTT) entities, as appropriate. To provide a foundation for such initiatives, DHS' Office of Infrastructure Protection coordinated the development of the NIPP along with its recent 2013 update. The NIPP is a government and industry-developed national plan that sets forth a comprehensive risk management framework and clearly defines the roles and responsibilities for DHS; Sector-Specific Agencies (SSA); and other Federal, SLTT, and private sector partners engaging in critical infrastructure protection (CIP) efforts.

3. **Membership, Working Groups, and Meetings**
   The IT GCC consists of representatives from across various levels of government, including Federal and SLTT entities, to enable interagency, intergovernmental, and cross-jurisdictional coordination within and across the Information Technology (IT) Sector. The IT GCC works with the IT Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed private sector council consisting of owners and operators and their representatives from across the sector's critical functions, including the provision of IT products and services, incident management capabilities, domain name resolution services, identity management and associated trust support services, Internet-based content, information, and communications services, and Internet routing, access, and connection services. The IT GCC/IT SCC partnership serves as the principal collaboration point between the IT Sector government and private industry members to effectively engage in sector-specific CIP policy, coordination, information sharing, and planning; cybersecurity; and risk management.

   The IT GCC reserves the right to invite participants from all levels of government to meet the expertise requirements necessary to fulfill any activity. SLTT representatives may join all IT GCC meetings and activities following approval from the IT GCC Chair. Federal departments and agencies should inform the Industry Engagement and Resilience (IER) Branch, which is part of CS&C's Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) Division and manages IT GCC activities, of their interest to join the IT GCC so that they can be formally recognized as official members. IER currently maintains the list of IT GCC members.

   IT GCC Working Groups are established when substantial investigation, research, or other tasks are required that cannot be achieved via regular IT GCC meetings. All IT GCC Working Group products are meant to advise IT GCC members on various issues and processes. The IT GCC Chair will designate Working Group Chairs and Co-Chairs either by nomination or through volunteering.

   The IT GCC Chair will convene IT GCC meetings, either in the form of in-person meetings or teleconference calls, on an as-needed basis.

4. **Scope**
   A collaborative and productive IT GCC is critical to building and maintaining beneficial partnerships, as well as developing useful and actionable products (e.g., analyses, reports, plans, etc.) that inform communications response, recovery, and risk management strategies and processes. The IT GCC actively pursues several types of activities, which include but are not limited to:

A. Identifying, prioritizing, and coordinating the IT Sector's CIP and resiliency activities with a range of public and private sector stakeholders;

B. Identifying needs and/or gaps in current IT-related CIP plans, programs, policies, procedures, and strategies, as well as measuring their effectiveness;

C. Promoting awareness of current IT Sector activities within the sector and across the other critical infrastructure sectors; and

D. Inviting Federal and SLTT representatives to share their experiences, ideas, best practices, and innovative approaches related to communication CIP and resiliency.

5. Roles and Responsibilities

The table below details the roles and responsibilities for each IT GCC component.

IT GCC Component	Roles and Responsibilities
DHS, CS&C, SECIR, IER	• Serve as the IT GCC Chair (as the CS&C-designated branch serving as the SSA for the IT Sector); • Facilitate the IT GCC's interaction and collaboration with the IT SCC; • Collect, discuss, and review NIPP-related issues from the IT SCC, IT GCC, and other Federal and SLTT department and agency representatives; • Initiate or bring issues to the IT GCC for consideration, deliberation, and resolution; • Establish an IT GCC leadership framework and process; • Provide meeting and organizational support, such as: – Coordinate meeting material development (e.g., agendas, summaries, etc.); – Support the IT GCC's efforts to monitor and close issues and initiatives; – Provide administrative and logistical support to the IT GCC (e.g., meeting room facility coordination, day-of meeting support, summary development, etc.); and – Promote information sharing through collaborative mechanisms, such as the DHS Homeland Security Information Network.
IT GCC Member	• Partner with the IT GCC Chair, CS&C, and other IT GCC members to develop strategic communications for CIP planning and coordination, and facilitate the discussion and resolution of CIP-related issues; • Enhance the foundation for protective programs with sector partners; • Lend subject matter expertise to the IT GCC to identify and prioritize sector challenges and risks; • Coordinate with, and support select efforts of, the IT SCC to plan, implement, and execute the Nation's IT CIP mission; • Participate in planning, developing, implementing, updating, and revising the IT Sector-Specific Plan and Sector Annual Report; and • Collaborate with private and public sector partners to share CIP-related information (e.g., experiences, best practices, lessons learned, etc.) within the IT Sector, as appropriate.

Signed: [redacted] Date: 2/8/2015

Christopher Duvall
Section Chief, IT and Communications Sectors
Industry Engagement and Resilience Branch
Office of Cybersecurity and Communications
Department of Homeland Security