**Information Technology**

**Sector Coordinating Council**

**Corporate Membership Application**

The primary mission of the IT SCC is to bring together companies, associations, and other key IT sector participants to discuss sector security issues and engage with the public and private sectors in all areas of critical infrastructure protection. Specifically, the IT SCC was established for the purposes of:

* Identification of IT sector critical infrastructure protection policy engagement topic areas.
* Consideration and publication of CIP policy positions addressing the integration of United States information technology infrastructure with the global information system.
* Integration of IT Sector CIP policy development with other industry sectors.
* Improving information sharing among the IT sector, government entities, sector members, and other industry sectors.
* Reviewing of and commenting on CIP-related plans and policies.
* Coordination between and among the sector’s policy-focused and operations-focused mechanisms, and their Government ordinates with regard to:
	+ Development of sector recommendations for preparedness and incident response and recovery plans based on the experience of members of the sector.
	+ Development of sound practices and lessons learned associated with respect to CIP.
	+ Identification of vulnerabilities, interdependencies, risk assessments and risk management methodologies (including vulnerability remediation and policy enforcement) with respect to CIP.
	+ Such additional purposes as the IT SCC Executive Committee may from time to time approve consistent with the foregoing purposes.

Kindly complete the information below and return to Angela McKay at angela.mckay@microsoft.com and Devon Snodgrass at v-desnod@microsoft.com. Thank you.

**Contact Information**

|  |
| --- |
| **Company Name:** Click here to enter text. |
| **Primary Company Address: Click here to enter text.** |
| **City:** Click here to enter text. | **State:** Click here to enter text. | **Zip:** Click here to enter text. |
| **Phone:** Click here to enter text. |
| **Website**: Click here to enter text. |
| **Primary Representative:** Click here to enter text. |
| **Title:** Click here to enter text. |
| **Address** |
| **Phone:** Click here to enter text. | **Email:** Click here to enter text. |
| **Additional Representative:** Click here to enter text. |
| **Title:** Click here to enter text. |
| **Address:** Click here to enter text. |
| **Phone:** Click here to enter text. | **Email:** Click here to enter text. |

*NOTE: as many additional representatives can be listed as desired*

|  |
| --- |
| **\*PR/Press Contact**: Click here to enter text. |
| **Title**: Click here to enter text. |
| **Address**: Click here to enter text. |
| **Phone**: Click here to enter text. | **Email**: Click here to enter text. |
| **\*Operations Center Contact**: Click here to enter text. |
| **Title**: Click here to enter text. |
| **Address**: Click here to enter text. |
| **Phone**: Click here to enter text. | **Email**: Click here to enter text. |
| **\*Crisis Communications Contact**: Click here to enter text. |
| **Title**: Click here to enter text. |
| **Address**: Click here to enter text. |
| **Phone**: Click here to enter text. | **Email**: Click here to enter text. |

**Please include a brief description of your organization, the organization website, and a statement identifying why you feel you should be a member of the IT SCC**:

**Working Group Participation**

The IT SCC asks that all Members participate in operating committees (Working Groups). Working Groups will be formed and disbanded according to a dynamic program. Currently there are six (6) Working Groups in operation.

Please check one or more of the working groups in which you would like to participate.

[ ]  ***International Committee*** –The group identifies areas for collective work between the IT (and Communications) Sectors and the U.S. Government (USG) on international cybersecurity and critical information infrastructure protection (CIIP) and assembles key subject matter experts to engage in pertinent activities. The goal is to share information on activities and policy developments, identify opportunities for engagement with countries or organizations, and develop substantive contributions to issues of mutual interest.

[ ]  ***Plans and Issues Working Group*** – The Plans and Reports Working Group consists of chairs from each of the IT SCC committees, and integrates the planning and reports received from each of the committees. This includes providing annual updates to National Infrastructure Protection Plan (NIPP) products such as the Sector Annual Report, Sector Specific Plan, Tier 1/Tier 2 data inputs, and the annual Strategic Homeland Infrastructure Risk Assessment (SHIRA) process.

[ ]  ***Policy Committee*** – The Policy Committee reviews public policy issues that affect the sector and makes recommendations to the IT SCC Executive Committee (EC) for action.

[ ]  ***Information Sharing Working Group*** – The IT Sector Coordinating Council (SCC) Information Sharing Working Group was formed to identify various information sharing programs sponsored by the federal government and to propose ways to streamline or consolidate these efforts with the goal of enhancing situational awareness among IT SCC members and federal partners.

[ ]  ***Supply Chain Working Group*** - The information technology (IT) sector’s supply chain is global, diverse, and interconnected. Evolving cyber-threats to networks, software, and system hardware present unique risks to users of IT, as well as to the producers of IT products that form the foundation of cyberspace and enable the global IT ecosystem. From software and hardware assurance and reliability, to intrusion and counterfeiting prevention, ensuring that the global IT supply chain is secure is an important element of the U.S. Government’s cyber security strategy and a priority for the IT industry. The IT SCC Supply Chain Working Group works with its government partners to provide industry input based on real-world experience regarding supply chain issues with the goal of ensuring that effective and efficient supply chain requirements for sensitive and high-assurance government IT systems are reflected in policy and guidance documents.

[ ]  ***Cross Sector Cybersecurity Working Group***

**Type of Information Technology Sector: (please select all that apply to your organization)**

[ ]  Domain Name System (DNS) root and Generic Top Level Domain (GTLD) operators

[ ]  Internet Service Providers (ISPs)

[ ]  Internet backbone providers

[ ]  Internet portal and email providers

[ ]  Networking hardware companies (e.g. fiber-optics makers and line acceleration hardware manufacturers) and other hardware manufacturers (e.g. PC and server manufacturers and information storage)

[ ]  Software companies

[ ]  Security services vendors

[ ]  Communications companies that characterize themselves as having an IT role

[ ]  IT edge and core service providers

[ ]  IT System integrators

[ ]  IT Sector Association

**Eligibility Criteria**

The IT SCC will accept for membership: (check which one applies)

[ ]  Any organization with significant business activity in any of the Information Technology Sector categories enumerated above or

[ ]  IT sector associations the membership of which is comprised significantly of entities or professionals and practitioners engaged in any IT activities listed above.

**What is the size of your company or association?**

[ ]  Small

[ ]  Medium

[ ]  Large

Revenue: Click here to enter text.

Number of Employees: Click here to enter text.

**What is your organization’s priority in critical information technology: (check all that apply):**

[ ]  Business continuity

[ ]  Risk assessment and management

[ ]  Cyber security

[ ]  Physical security

[ ]  Compliance

[ ]  Threat analysis

[ ]  Crisis Communication

[ ]  Other (please list): Click here to enter text.

**How did you learn about the IT SCC?**

[ ]  Referred by IT SCC member (identify company and individual): Click here to enter text.

[ ]  IT SCC Website

[ ]  Press/News (please specify source): Click here to enter text.

[ ]  Other (please specify): Previous engagement with IT-SCC

**Any other comments:**

Click here to enter text.

Please send all applications to Angela McKay at angela.mckay@microsoft.com and Devon Snodgrass at v-desnod@microsoft.com. Thank you.