CSCC

U.S. Communications
Sector Coordinating Council

INFORMATION TECHNOLOGY
IT
SCC
SECTOR COORDINATING COUNCIL ™

Communications Sector and Information Technology Sector

Presentation to NANOG

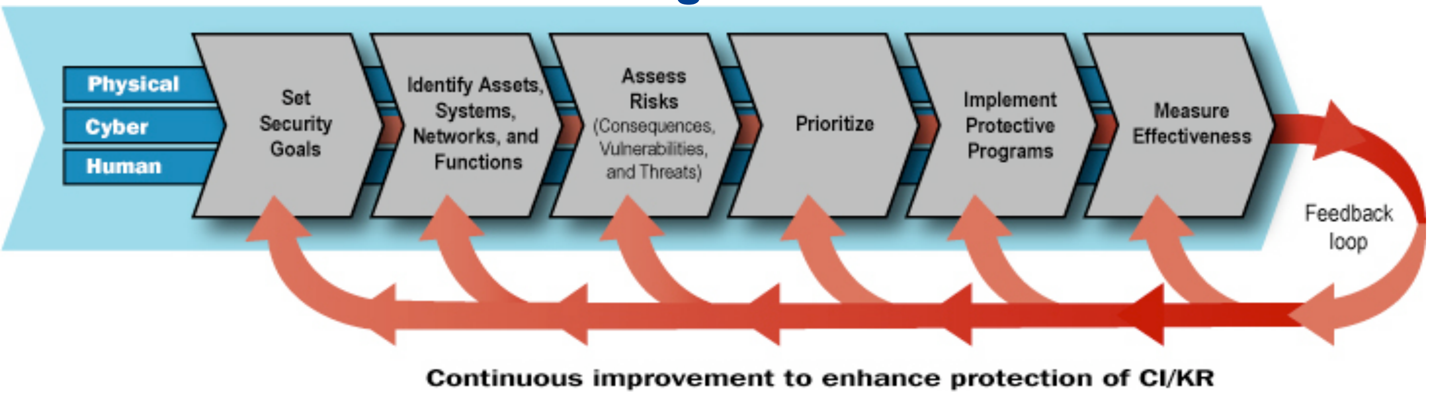
June 15, 2009

Marcus H. Sachs, Verizon
Jared Mauch, NTT America

U.S. National Infrastructure Protection Plan (NIPP)

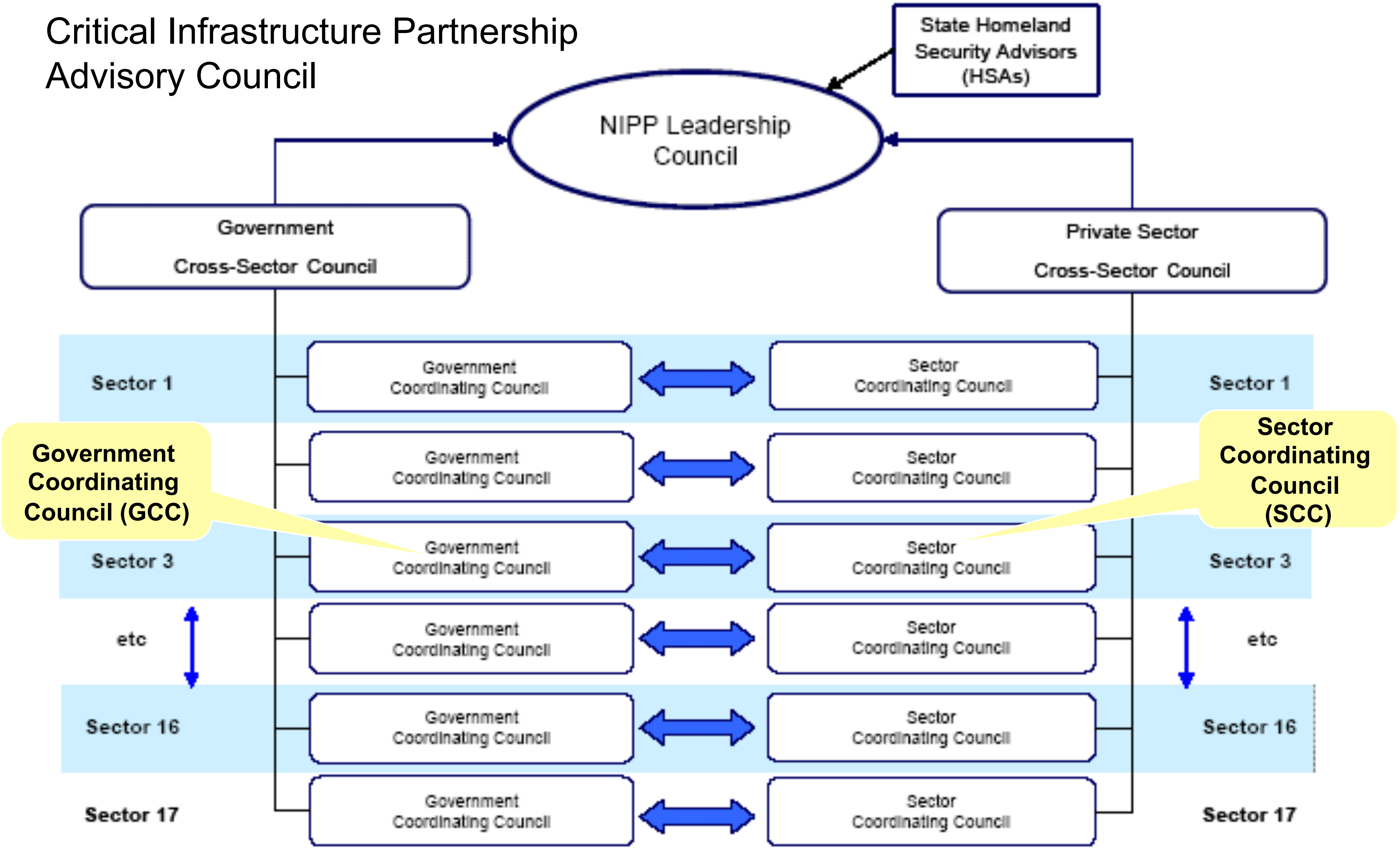
- Outlines a structure for U.S. critical infrastructure protection
- Provides the framework for all levels of U.S. government to collaborate with appropriate security partners, including private sector entities
- Consists of a base plan and 18 sector-specific plans to cover all areas of critical infrastructure and key resources (CI/KR) as identified in U.S. Homeland Security Presidential Directive 7 issued by the President in 2003
- Describes responsibility to address physical, human, and cyber risk in all infrastructure sectors

NIPP Risk Management Framework


Physical
Cyber
Human
Set Security Goals
Identify Assets, Systems, Networks, and Functions
Assess Risks (Consequences, Vulnerabilities, and Threats)
Prioritize
Implement Protective Programs
Measure Effectiveness
Feedback loop
Continuous improvement to enhance protection of CI/KR

The NIPP can be accessed at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

NIPP Partnership Structure



Critical Infrastructure Partnership Advisory Council

State Homeland Security Advisors (HSAs)

NIPP Leadership Council

Government Cross-Sector Council

Private Sector Cross-Sector Council

Government Coordinating Council (GCC)

Sector Coordinating Council (SCC)

Sector 1

Government Coordinating Council

Sector Coordinating Council

Sector 1

Government Coordinating Council

Sector Coordinating Council

Sector 3

Government Coordinating Council

Sector Coordinating Council

Sector 3

etc

Government Coordinating Council

Sector Coordinating Council

etc

Sector 16

Government Coordinating Council

Sector Coordinating Council

Sector 16

Sector 17

Government Coordinating Council

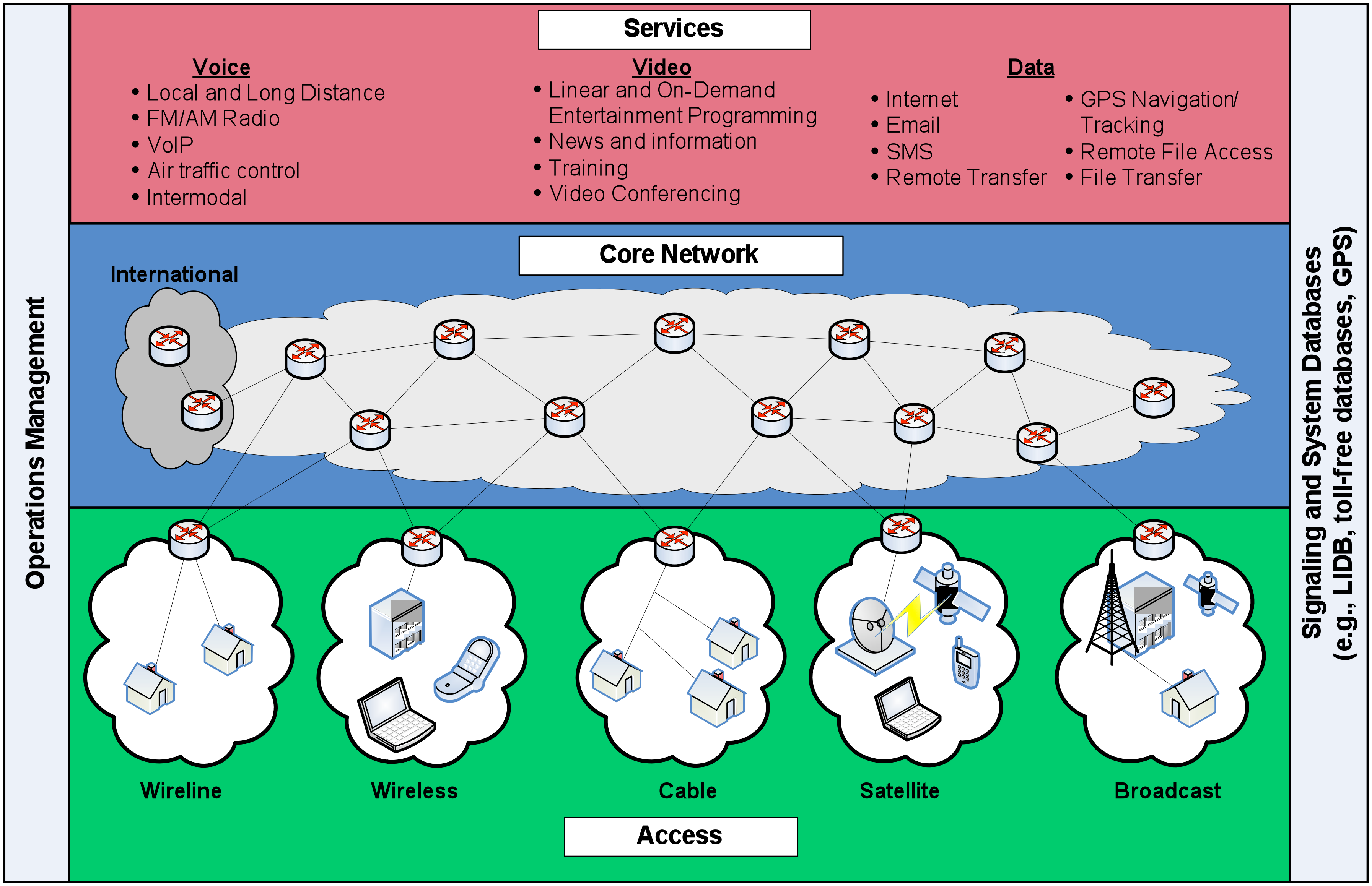
Sector Coordinating Council

Sector 17

NIPP Accomplishments and Deliverables

- IT Sector Specific Plan was the first plan jointly written by government and industry; reflects needs of both sets of stakeholders
- Completely overhauled how government views IT risk methodology to reflect market realities (e.g. the IT Sector identifies function-based risks vs. asset-based risks)
- Plan identifies security goals and specific initiatives to meet them; agreed to by both public and private sector

Communications Sector Overview



Operations Management

Services

Voice

- Local and Long Distance
- FM/AM Radio
- VoIP
- Air traffic control
- Intermodal

Video

- Linear and On-Demand Entertainment Programming
- News and information
- Training
- Video Conferencing

Data

- Internet
- Email
- SMS
- Remote Transfer
- GPS Navigation/ Tracking
- Remote File Access
- File Transfer

Core Network

Access

Signaling and System Databases (e.g., LIDB, toll-free databases, GPS)

National Security/Emergency Preparedness Cooperation

- National Communications System (NCS)
  - Established by President Kennedy in 1963
  - ***Sector Specific Agency*** for the Communications Sector
  - Today is part of the Department of Homeland Security's National Cyber Security and Communications Division
- National Coordinating Center for Telecommunications (NCC) and Comm-ISAC
  - Established in 1984 as a central public-private sector organization to coordinate response to emergency communications situations
  - Information Sharing and Analysis Center for Telecommunications
  - ***Operational component*** of the Communications Sector
  - Collocated with the US-CERT in Arlington, Virginia

National Security/Emergency Preparedness Cooperation (continued)

- National Security Telecommunications Advisory Committee (NSTAC)
  - Established in 1982
  - Advisory committee to the President
  - Policy component of the Communications Sector
  - 30 industry chief executives representing major telecommunications companies, network providers, information technology companies, finance, and aerospace businesses
- Communications Sector Coordinating Council (CSCC)
  - 42 member companies include wireline, wireless, cable, satellite, information service providers, commercial and public broadcasters, service integrators, equipment vendors, and private, internal networks that support core services/operations
  - Planning component of the Communications Sector
  - Small and medium size companies are represented through CTIA, USTelecom, ITA and NCTA

Communications Sector Coordinating Council

- Meets quarterly to review industry and government actions on critical infrastructure protection priorities and cross sector issues
  - Executive Committee meets monthly
- Coordinates with industry participants in the NSTAC and the Comm-ISAC (NCC)
- Coordinates with other sectors through
  - Partnership for Critical Infrastructure Security (PCIS)
  - Cross Sector Cyber Security Working Group (CSCSWG)
  - Industrial Control Systems Joint Working Group (ICSJWG)
  - National Level Exercises (NLEs)

2009 C-SCC Priorities

- Partnering with the IT sector on cyber security
  - Participation in the Cross Sector Cyber Security Working Group
  - Support for executing the President's Cyber Initiative and the White House 60-day review of cyber security policies
  - Assisting the IT-SCC with their risk assessment as needed
- Infrastructure resiliency and risk-management practices
  - Wireless protocols for service shut-down and restoration
  - Access and credentialing
  - Regionalization of Communications Support
- Programmatic metrics and sector-specific metrics
- Updating the public web site (http://www.commscc.org)
- Consulting with government representatives and organizations and private sector entities to ensure appropriate exchanges of information to enhance key policy work such as:
  - SHIRA threat analysis
  - National Emergency Communications Plan (NECP)
  - NIPP and SSP reviews/updates
  - Cross-sector dependency studies

C-SCC Coordination with the IT-SCC

- Both sectors participate actively in the PCIS Cross Sector Cyber Security Working Group
- Both have worked to heighten industry's role in NS/EP exercises such as last year's ESF2 exercise, TopOff 4, and CyberStorm
- Both sectors were well represented on the CSIS Commission on Cyber Security for the 44th Presidency, various CNCI efforts including the development of "Project 12", and assisting the White House with a 60-day review of cyber security policies
- Both organizations have designated sector liaisons to attend each other's coordinating council meetings
- Both meet annually in a joint session to confer with government counterparts on ongoing sector activity

Communications Sector Additional Resources

- Communications SCC
  - http://www.commscc.org
- Communications Sector-Specific Plan
  - http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf
- Communications ISAC
  - http://www.ncs.gov/ncc
- National Communications System
  - http://www.ncs.gov
- National Security Telecommunications Advisory Committee (NSTAC) Publications
  - http://www.ncs.gov/nstac/nstac_publications.html

IT Sector Coordinating Council (IT SCC) Overview

What is the IT SCC?

- Information Technology Sector Coordinating Council, established on January 27, 2006
- Vision: A secure, resilient, and protected information infrastructure.
- Mission:
  - To ensure continued, resilient and efficient functioning of information technologies, infrastructures and services for people, governments, and businesses worldwide,
  - To bring together companies, associations, and other key IT sector participants on a regular basis to coordinate strategic activities and debate and communicate sector member views associated with infrastructure protection, response, recovery and risks that are broadly relevant to the IT Sector, and
  - To work with DHS, other government stakeholders and other sectors on policy issues related to the IT sector and critical infrastructure protection.

Who can join the IT-SCC?

- Must be an owners and operators of IT and Internet Infrastructure or IT associations with significant business activity representing the IT Sector including:
  - 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

Why is the IT SCC important to maintain?

- Trusted legal framework (CIPAC); provides legal protection for ongoing, strategic collaboration on policy issues between industry and government
- IT SCC seen as “partner”, not group of “vendors”; companies have put significant time and resources investing in this model, which is beginning to bear fruit
- IT SCC membership: XX% of the IT Sector market share
  - Consolidated sector organization for government to share information, collaborate on policy and strategy affecting IT sector, interdependencies between sectors (e.g. CNCI Project 12, Protective measures, etc)

IT SCC Strategic Objectives

- Create a framework for government and private sector to work together to address risk to the IT sector and nation
- Create a dynamic and informed assessment of cyber and physical risk to the IT sector, as well as interdependencies to other sectors
- In concert with the IT-ISAC, develop a public-private capability for situational awareness, analysis, response and recovery
- Develop a joint national R&D plan affecting IT sector for government

Priorities and Activities to date

- NIPP Framework, IT Sector Specific Plan, and IT Risk Assessment
- Protective Programs and Research & Development Project (e.g., development of R&D agenda)
- Comprehensive National Cyber Initiative Projects
- Collaboration with IT ISAC, Comms SCC, Cross Sector Cyber Working Group (CSCSWG) and other groups

IT Sector Risk Assessment Accomplishments and Deliverables

- Functions-based risk assessment model to more accurately reflect how sector operates
- Identified six critical functions within the IT Sector
- Development of attack scenarios to apply and assess risks to each function
- Detailed risk assessment methodology enables us to manage risks and identify protective programs and R&D requirements.

This all leads to real, actionable information for the sector and government to manage risks and more effectively protect critical infrastructure

CNCI Accomplishments and Deliverables

- Completed joint work on Project 12 report with Dept of Homeland Security (IT GCC)
- Continue to provide input into the Initiative through various projects and working groups

IT-SCC Coordination with the IT-ISAC

- The IT-ISAC is the IT SCC designated (and DHS recognized) operational arm of the sector (e.g. information sharing, incident response, threat and vulnerability analysis). The IT-SCC is the policy arm of the sector;
- IT-ISAC is a standing member of the IT-SCC and designates a permanent representative on the IT-SCC Executive Committee.
- The IT-ISAC provides valuable technical analytical capability, sharing information related to the health of the information infrastructure.
- In areas of operational policy, the IT-SCC and IT-ISAC coordinate closely; (e.g. Cyber Storm, TOPOFF and the IT ISAC CONOPS)
- The IT-ISAC shares information regularly with IT SCC members

IT-SCC Coordination with the Comms-SCC

- Both IT and Comms jointly own/operate the Internet infrastructure
- Both SCC's organizations have elected ex-officio representatives to attend and participate in each other's coordinating council meetings and Executive Committee sessions; reflects industry convergence and ensures coordination between the two sectors
- IT and Comms meet jointly to confer with government counterparts on ongoing sector activity, preparation and response to major incidents.
- Both sectors participate in a recently formed cross sector cyber security working group (CSCWG)
- Both have worked to heighten industry's role in NS/EP exercises such as last summer's ESF2 exercise in New Orleans and in TopOff 4
- Both participate in ongoing sector risk assessments

Where can more work be done?

- R&D
- Cyber Storm: further execution from lessons learned
- Stop writing new plans; spend time implementing existing plans and risk assessments across sectors

Add’l IT-SCC membership eligibility requirements?

- Must participate in quarterly plenary sessions (should not miss more than two sessions per year)
- Must participate in at least one operating Working Group. The current Working Groups in operation are:
- **Communications and Outreach Working Group:**
  - Chair: Franck Journoud of the Business Software Alliance
  - Recruitment and retention of members is a core function of this group, working with the IT SCC Secretary to activate new members. This group also creates and maintains all communications media, including the ITSCC “101 presentation”, the IT Sector Scorecard, and the website. Additional efforts include outreach across other organizations to spread awareness of IT SCC activities and accomplishments.

Add’l IT-SCC membership eligibility requirements?

- **Plans and Reports Working Group:**
  - Chair: Ken Watson of Cisco
  - 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.
- **Risk Assessment Committee:**
  - Chair: Scott Algeier of the IT-ISAC
  - The Risk Assessment Committee developed and is completing the initial comprehensive Sector Baseline Risk Assessment. The committee’s next step is to map out a plan for raising awareness about the assessment, and a process to regularly update the Sector Risk Assessment.

Add'l IT-SCC membership eligibility requirements?

- **Information Sharing Committee:**
  - Co-Chairs: John Lindquist of EWA-IIT & Roland Cloutier of EMC
  - The Information Sharing Committee will work to develop an Information Architecture that will fill the needs of: 1) owners and operators of critical IT Infrastructures; and 2) the IT SCC and its committees. In the first case, the committee will address in a general way the information needs to conduct risk assessments, prepare protection and response plans, maintain situational awareness during an incident, and restoration of the functional capability or services. The architecture will attempt to define the types of information needed, the potential sources for that information, and a collection and dissemination management construct so that owner/operator needs are fulfilled. In the second case, the committee will address an architecture to fulfill information needs of the IT SCC in it policy and coordination role. This will include awareness of current government policy and intent, status of ongoing programs, and notification of specific policy or coordination requirements. The intent is to develop a system that will allow informed discussion with government and other sector counterparts as well as a process within the IT SCC to facilitate arrival at an informed consensus on the IT SCC positions vis a vis those discussions.

Add’l IT-SCC membership eligibility requirements?

- **Metrics Committee:**
  - Co-Chair: Clint Kreitner of the Center for Internet Security and Mike Gibbons of Deloitte and Touche LLP.
  - The Metrics Committee is focused generally on developing metrics that will be used to express the effectiveness of the cybersecurity-enhancing activities included in the It Sector Specific Plan. A specific focus will be on devising metrics that measure how effectively the critical functions and sub-functions are mitigating the risks reported in the IT Sector Baseline Risk Assessment.
- **Protective Programs Committee:**
  - Co-Chairs: Ed White of McAfee and Ryan Walters of Northup Grumman
  - The Protective Programs Committee focuses on identifying new and enhanced capabilities to prepare for, protect against, respond to, and recover from incidents that have the potential to impact critical IT Sector functions. The work consists of mapping current IT Sector protective program capabilities to government protective programs to analyze their effectiveness, relevance, and redundancy, as well as to perform a gap analysis to determine future protective program requirements recommended in the Sector Annual Report.

Add’l IT-SCC membership eligibility requirements?

- **Research and Development Committee:**
  - Co-Chairs: Brent Williams of Anakam and Saadat Malik of Cisco
  - The IT Sector R&D Committee’s vision is to create a partnered environment that allows both Government and private sector to collaborate on IT Sector critical infrastructure/key resources R&D. One of the primary focus areas for the group is to examine the range of public and private cyber security R&D initiatives and help guide the Government’s focus towards R&D projects that have limited financial viability for the commercial sector. The committee seeks to develop and execute on a process through which the private sector is incentivized to effectively share relevant information around its R&D efforts with the government, a gap analysis is conducted on this information to understand what areas of R&D are critical to national security and are not getting due attention in the private sector and, finally, recommendations for areas of R&D to focus on are developed and delivered to organizations inside the government where they can be most effectively implemented. This group will be informed by the outcomes of the IT Sector Baseline Risk Assessment and will work collaboratively with the Protective Programs Committee.

IT-SCC Executive Committee Composition

- Executive Committee Composition
  - Two Designated Positions for the IT-ISAC and the Communications-SCC
  - Three Sponsored Association Positions
  - Seven At-Large Industry Owner/Operator Positions
- More information about the process for becoming a IT-SCC Executive Committee member can be found at www.itscc.org

How does my organization become an IT-SCC member?

- Complete a membership application and return to liesyl_franz@techamerica.com and andrew_mclaren@sra.com
- Membership will be vetted by the Executive Committee and voted on by IT-SCC membership

CSCC

U.S. Communications
Sector Coordinating Council

INFORMATION TECHNOLOGY
IT
SCC
SECTOR COORDINATING COUNCIL ™

Communications Sector and Information Technology Sector

QUESTIONS?

Marcus H. Sachs, Verizon
Jared Mauch, NTT America