



# Partnership for Critical Infrastructure Security, Inc. (PCIS)

## Update for CIP Congress

Ken Watson

October 18, 2006

[kwatson@cisco.com](mailto:kwatson@cisco.com)

# Agenda



*The “partnership framework” is in place*

- ◆ Critical Infrastructure Partnership Advisory Council (CIPAC)
  - ❖ What is it ?
  - ❖ Who is on it ?
  - ❖ Why do we need it ?
- ◆ Partnership for Critical Infrastructure Security, Inc. (PCIS)
  - ❖ What is it ?
  - ❖ How does it relate to CIPAC and the ISAC Council ?
  - ❖ Update on initiatives

# Critical Infrastructure Partnership Advisory Council (CIPAC)



- ◆ Established March 2006 by Secretary, DHS to:
  - ❖ Facilitate strategic planning and effective discussion of critical infrastructure issues;
  - ❖ Protect sensitive critical infrastructure information; and also
  - ❖ Observe appropriate public disclosure procedures for the council.
- ◆ “Effective critical infrastructure protection requires the ability to have **real time, continuous communications** and **open dialogue** among the public and private partners in the model. The granting of the 871 exemption will establish a known and understood framework that **facilitates the flow of advice and information** concerning critical infrastructure protection. Not doing so would inhibit information sharing, risk publicly disclosing vulnerabilities, and suppress ad hoc communications during emergencies.”

--Federal Register, March 24, 2006 (Volume 71, Number 57)] [Notices]  
[Page 14930-14933]

# CIPAC Charter



- ◆ Facilitate more effective coordination of Federal infrastructure protection programs with infrastructure protection activities of private sector and of State, Local, territorial, and tribal governments.
- ◆ The range of activities includes planning, coordination, security program implementation, and operational activities related to critical infrastructure protection security measures, including incident response, recovery, and reconstitution.

## Among Other Tasks, CIPAC...



- ◆ Supports implementation of the National Infrastructure Protection Plan (NIPP) and help effectuate the sector-partnership model
- ◆ Facilitates regular, ongoing, multi-directional communication and coordination between critical infrastructure and key resource (CI/KR) owners and operators and government
- ◆ Provides policy advice as it emerges (from above)

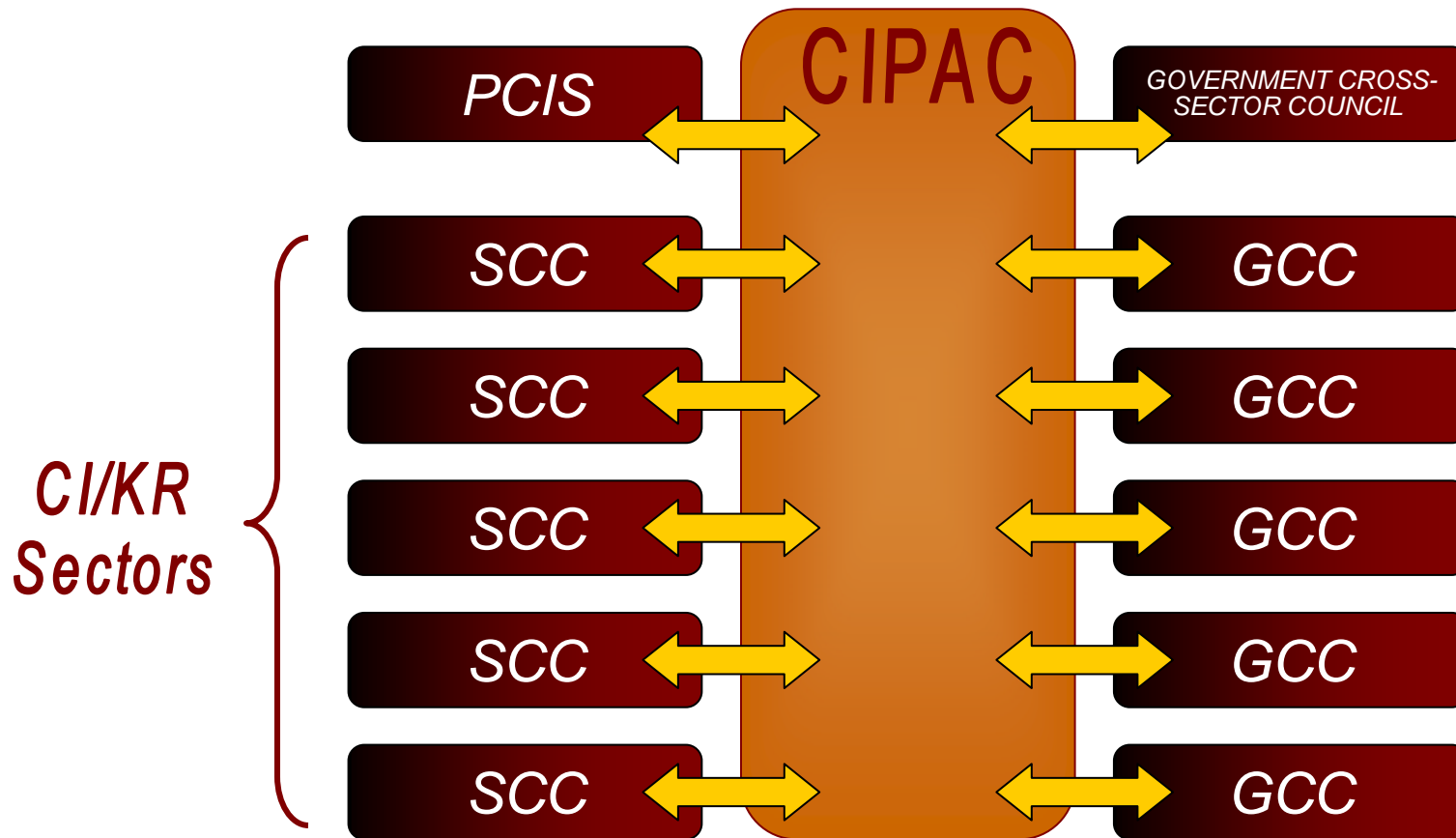
# CIPAC Composition



- ◆ CI/KR owners and operators that are **members of** their respective sector's recognized Sector Coordinating Council (**SCC**), **including** their representative **trade or equivalent organizations**
- ◆ Federal, State, local, and tribal governmental entities comprising the **members of** the Government Coordinating Council (**GCC**) for each sector, **including** their representative **trade or equivalent organizations**

# Sector-Partnership Framework

## Critical Infrastructure Partnership Advisory Council (CIPAC)



# “Lanes in the Road” Comparison



	<b>ISAC Council</b>	<b>PCIS</b>	<b>CIPAC</b>
<b>Members</b>	3 representatives per Information Sharing and Analysis Center (ISAC)	SCC representatives	SCC/GCC members (organizations)
<b>Purpose</b>	Facilitate consensus building, sharing information/best practices cross-sector and Situation Reports (SITREPs)	Coordination	Facilitate consensus building and dialog between owner/operators and government
<b>Scope</b>	Operational issues for sectors and cross-sector interdependencies	Cross-sector coordination, policy/strategy	Coordination and advice to DHS, Sector-Specific Agencies (SSAs)
<b>Public/Private</b>	Private	Mostly Private, except for Emergency Services and Postal Shipping SCCs	Public/Private



***PCIS***

**PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY**

# PCIS Mission Statement



Coordinate cross-sector initiatives and complement public-private efforts to promote and assure reliable provision of critical infrastructure services in the face of emerging risks to economic and national security

# History



- ◆ Formed December 1999 on invitation from Secretary of Commerce
- ◆ Ken Watson, founding President and Chairman
  - ❖ Board included designated Sector Coordinators and Corporate CIP owners/operators
- ◆ Five initial working groups:
  - ❖ National Plan
  - ❖ Research & Development
  - ❖ Information Sharing
  - ❖ Public Policy
  - ❖ Operations
- ◆ Early work:
  - ❖ Identified need to protect private-sector vulnerability information shared with government—resulted in PCII
  - ❖ Coordinated development of private-sector appendix to original National Strategy to Secure Cyberspace (July 2002)

# Composition



- ◆ PCIS members are the **sector coordinating councils**, represented by their chair, co-chair or other appointed individual.
- ◆ Individuals are **appointed** to PCIS representation **from** their **sectors**.
- ◆ Currently, PCIS selects its membership from government-recognized sector coordinating councils.
- ◆ ISAC Council Chair participates (non-voting)



## Current Sector Representation

- ◆ Banking and Finance
- ◆ Chemical
- ◆ Commercial Facilities
- ◆ Communications
- ◆ Dams, Locks, and Levees
- ◆ Emergency Services
- ◆ Energy – Electricity
- ◆ Energy – Oil and Natural Gas
- ◆ Food and Agriculture
- ◆ Healthcare
- ◆ Information Technology
- ◆ Nuclear
- ◆ Postal and Shipping
- ◆ Transportation – Railroad
- ◆ Public Transit
- ◆ Water

## Roles



- ◆ Encouraging and participating in public/private partnership with the Federal government over past **six years**.
- ◆ PCIS members are also **members of the CIPAC**.
- ◆ Focus: **cyber and physical** cross-sector critical infrastructure protection **policy and strategy** and **interdependency** issues of concern to the private sector.
- ◆ Improving the security and safety of the nation's critical infrastructures by **providing the forum** for critical infrastructure **sectors** to work among themselves as well as work in partnership with the Federal government.
- ◆ Formally recognized as the **Private-Sector Cross-Sector Council** in the National Infrastructure Protection Plan (NIPP), released in June 2006.

# Recent and Continuing Activities



- ◆ PCIS Governing Principles for Information Sharing
  - ❖ Developed as a **guide for the private sector** to build cross-sector information sharing capabilities
  - ❖ **Policy-level** description of the **need to share** information through secure and effective collection, analysis, and dissemination processes
- ◆ Addressing issues of common concern among the sectors
  - ❖ **Coordination of exercise planning** and other outreach efforts with Department of Homeland Security (DHS)
  - ❖ Protected Critical Infrastructure Information Program (**PCII**) **improvements**
  - ❖ Analysis of **cross-sector R&D gaps and priorities**
- ◆ Continual dialogue with DHS on emerging issues
  - ❖ **Credentialing** of private sector employees for emergency restoration work
  - ❖ **Pandemic** planning
  - ❖ **NIPP and Sector-Specific Plan (SSP)** development and implementation

# Strategic Focus Going Forward



- ◆ More proactive leadership on CIP issues and policy
- ◆ Improve communication and coordination
- ◆ Increase value to SCCs and sectors
- ◆ Strengthen role in cross-sector issues
- ◆ Strengthen effectiveness of PCIS organization

# Contact Information



- ◆ Chairman  
Stuart Brindley  
Manager - Training &  
Emergency Preparedness  
Independent Electricity  
System Operator (IESO)  
Ontario, Canada  
[stuart.brindley@ieso.ca](mailto:stuart.brindley@ieso.ca)  
905-855-6108
  - ◆ Secretary/Treasurer  
Dan Bart  
Senior Vice President, Standards  
and Special Projects  
Telecommunications Industry  
Association  
[dbart@tiaonline.org](mailto:dbart@tiaonline.org)  
(703) 907-7703
  - ◆ Vice Chairman  
Mike Wallace  
President, Constellation  
Generation Group  
Executive Vice President,  
Constellation Energy  
[mjw@constellation.com](mailto:mjw@constellation.com)  
410-782-2877
  - ◆ Executive Director  
Kathryn Condello  
[kcondell@gmu.edu](mailto:kcondell@gmu.edu)  
703-993-4861
- Web site: [www.pcis.org](http://www.pcis.org)

# Discussion

