A (very brief) Overview of US Information Sharing Policies

ENISA Workshop

March 16, 2010

Agenda

About the IT-ISAC

Information Sharing Policies and Tools

Progress and Challenges

The Road Ahead

About the IT-ISAC

IT-ISAC Mission

- **Share:** Report, exchange and analyze across the IT Sector information on electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures

- **Trust:** Establish a mechanism for systematic and protected exchange and coordination of the Information and trusted collaboration;

- **Lead:** Provide thought leadership to policymakers on cyber security and information sharing issues.

Members

Foundation Members

BAE Systems, IT

CA

Cargill, Inc.

CSC

eBay

EWA, IIT

IBM

Intel Corporation

Microsoft Corp.

Oracle USA, Inc.

SRA International

Symantec Corp.

VeriSign, Inc.

Silver Members

Cisco Systems, Inc.

Juniper Networks

McAfee, Inc.

NeuStar

Bronze Members

Prescient Solutions

USi

Information Sharing Policies and Tools

Scope of Problem

- Reliance on information technology for virtually everything from military to banking to electricity
- Information Technology is woven throughout modern society making us dependent on it for almost everything
- Basic building blocks/protocols are insecure
- Bad actors exploit flaws in technology and in human behavior for their advantage
- Actors are complex and often well financed
- Goals range from data theft and espionage to financial gain and economic chaos
- Neither industry or government have the capacity to meet these challenges alone

Policy of Collaboration

Industry

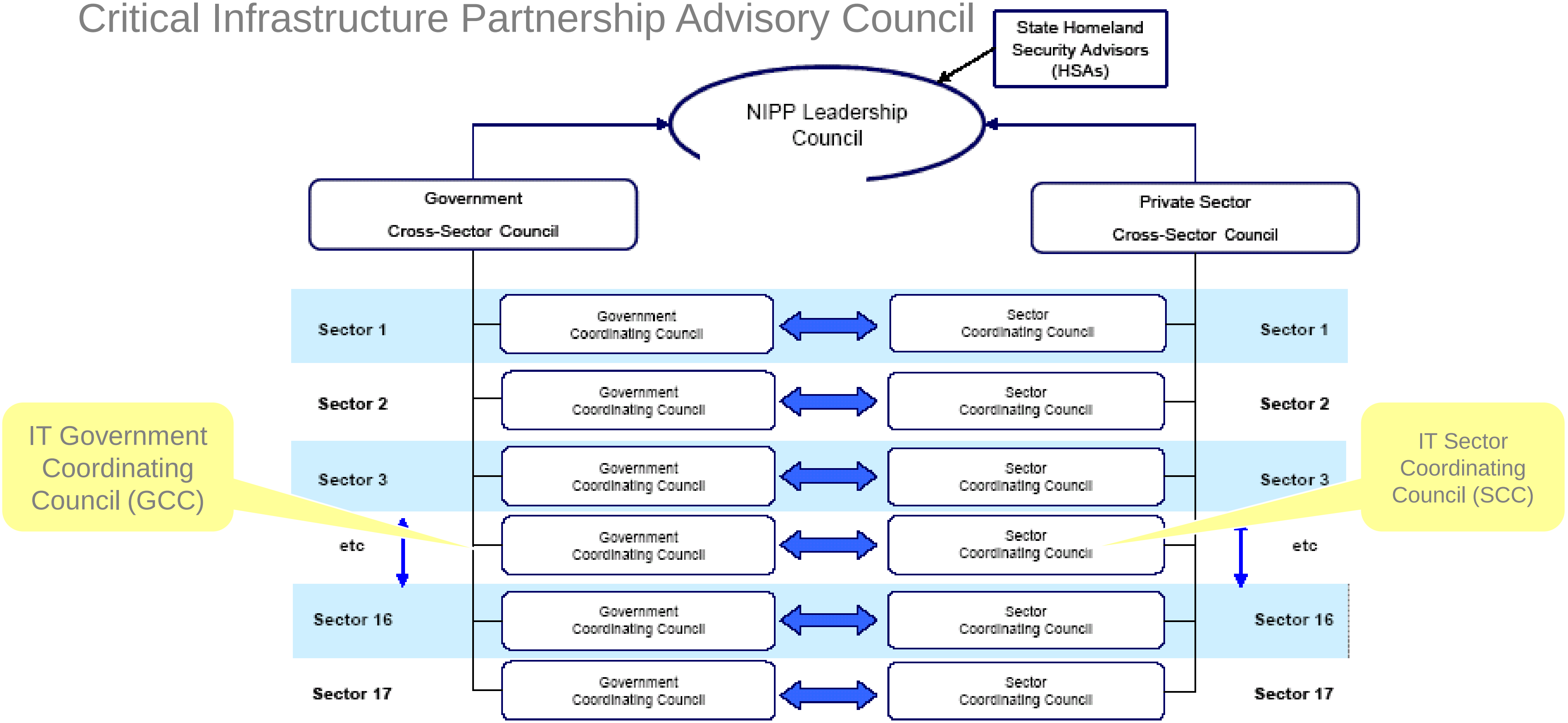
- Attacked every day
- Provides products and services, manages networks, maintain core internet protocols
- Has technological and intellectual tools often lacking in government
- Addresses the issue in many ways from an economics perspective (balance security investments with other business considerations)
- IT Sector either has the patch for the vulnerability of provides updates for more effective defenses
- Government will act anyway

Government

- Attacked every day
- Intelligence information on actors, threats, vulnerabilities and attack methods
- Often looked to by population for leadership in crises
- Addresses the issue as a security problem
- Informed decision making

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

Sector 1 — Government Coordinating Council ⟷ Sector Coordinating Council — Sector 1

Sector 2 — Government Coordinating Council ⟷ Sector Coordinating Council — Sector 2

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

IT Government Coordinating Council (GCC)

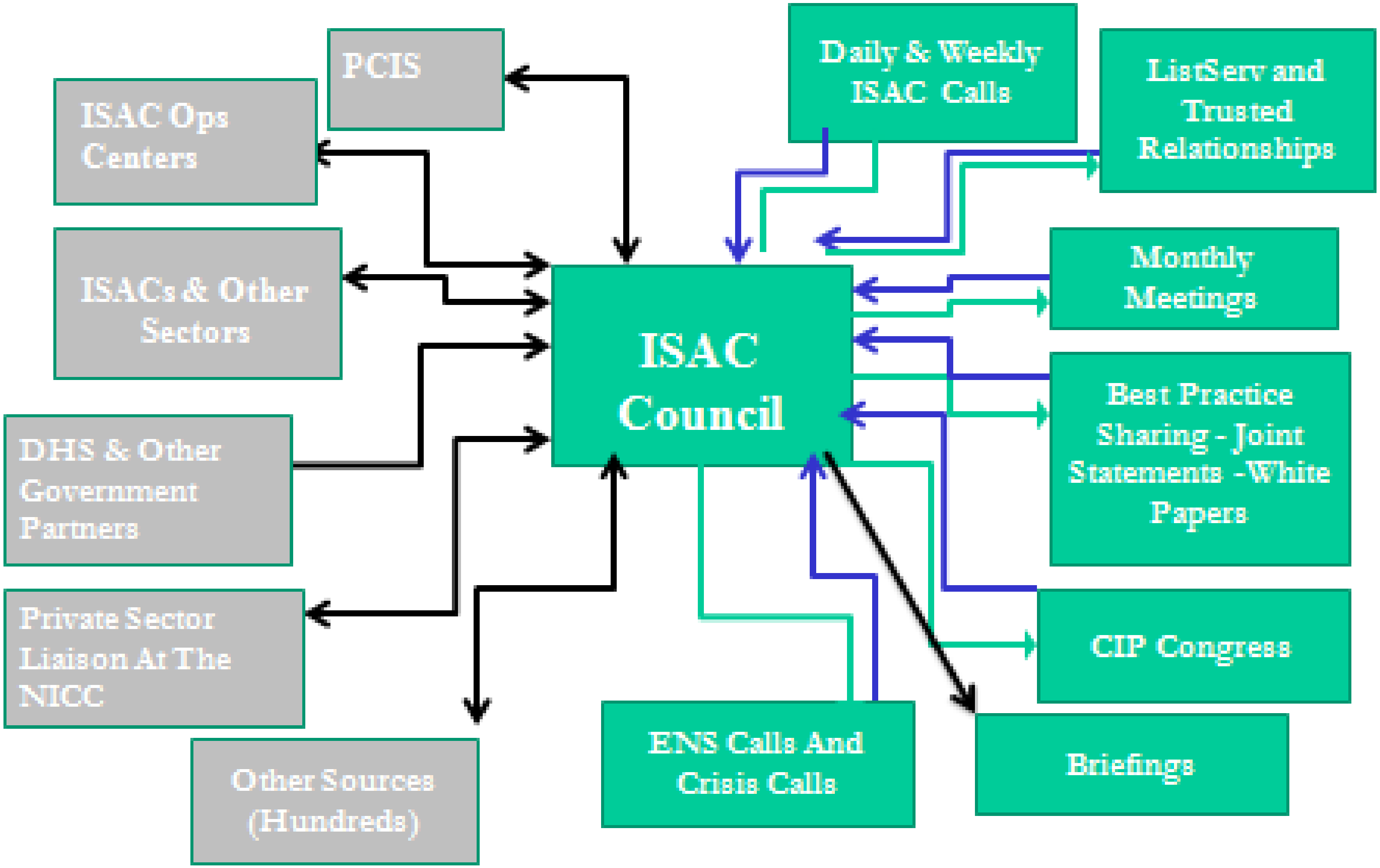
IT Sector Coordinating Council (SCC)

Available Information Sharing Tools

- Information Sharing and Analysis Centers
- Homeland Security Information Network
- US Computer Emergency Readiness Team
- InfraGuard
- Electronic Crimes Task Forces
- Fusion Centers
- Regional Consortiums
- Alerting systems

Information Sources

Communications



PCIS

ISAC Ops Centers

ISACs & Other Sectors

DHS & Other Government Partners

Private Sector Liaison At The NICC

Other Sources (Hundreds)

ISAC Council

Daily & Weekly ISAC Calls

ListServ and Trusted Relationships

Monthly Meetings

Best Practice Sharing - Joint Statements -White Papers

CIP Congress

Briefings

ENS Calls And Crisis Calls

Progress and Challenges

Information Sharing Progress

- Moving from a sharing information is dangerous culture to a “need to share” culture
- Developing a better understanding of who to share information with and how to get it to them
- Respecting the concept of originator control and developing methods to protect shared information
- Slowly understanding that “information sharing” is a tool, not the goal

Information Sharing Challenges Beyond “Legal” and “Trust”

- Classification
  - Private Sector Clearance Program
  - Review of FOUO
- Agency control
  - It remains difficult to change culture at institutions that are built on secrecy
  - DHS Depends on other agencies for information
- Disclosure
  - All it takes is one leak to cut off information sharing
  - Balance between broadcasting information and sharing with communities
- Information Needs
  - Each organization has its own needs
  - We’ve not collectively defined what information we need
  - Strategic vs. operational information

The Road Ahead

- Define the end state to drive information sharing requirements:
  - Securing the “sector” and the enterprise have different information requirements
  - Risk based information sharing
  - International partners

- Stronger cross sector coordination
  - Integrate the operational capabilities of the federal government, IT and Communications Sectors through co-location and building joint response capabilities.

- Streamline information sharing by using existing capabilities

- Bend the “cost benefit” curve to the benefit side
  - Too much risk and not enough reward in information sharing

The Business Case for Collaboration

"Cyber security is now one of the most important national security challenges facing the U.S. This is not some hypothetical catastrophe. We are under attack and taking damage."

Jim Lewis, Director and Senior Fellow Center for Security and International Studies, September 16, 2008. Testimony before House Subcommittee on Emerging Threats, Cyber Security and Science and Technology

IT-ISAC Contact Information:

Scott C. Algeier, Executive Director

salgeier@it-isac.org

703-385-4969--Direct

www.it-isac.org