DHS – DOD SOFTWARE ASSURANCE FORUM

FEBRUARY 28, 2011 – MARCH 4, 2011
MITRE
MCLEAN, VIRGINIA

Partnership for Critical Infrastructure Security

“ The role of the public – private partnership in critical infrastructure preparedness and resiliency”

March 3, 2011

NATIONAL INFRASTRUCTURE PROTECTION PLAN (NIPP)

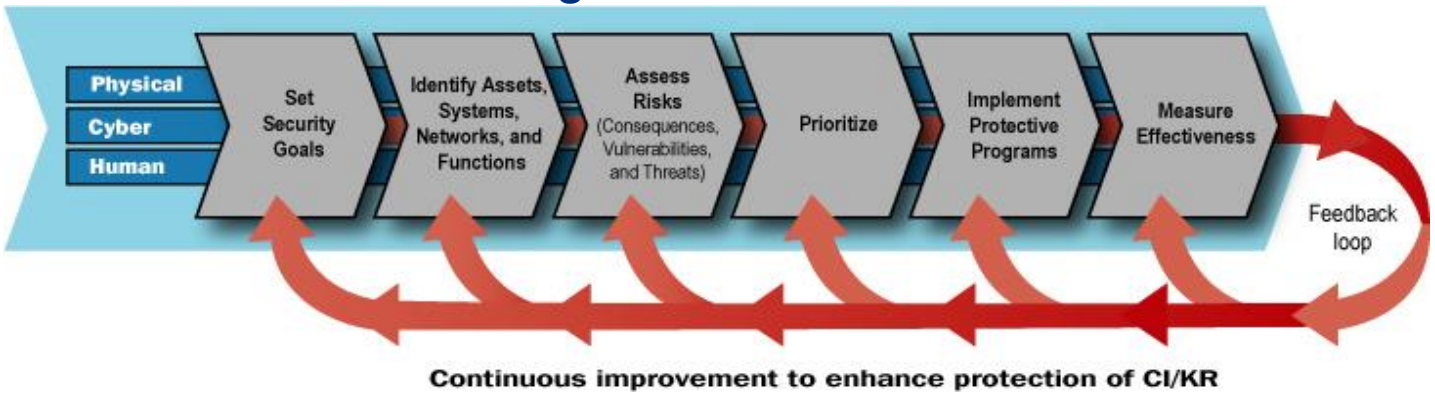
Outlines a structure for U.S. critical infrastructure protection

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 17 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

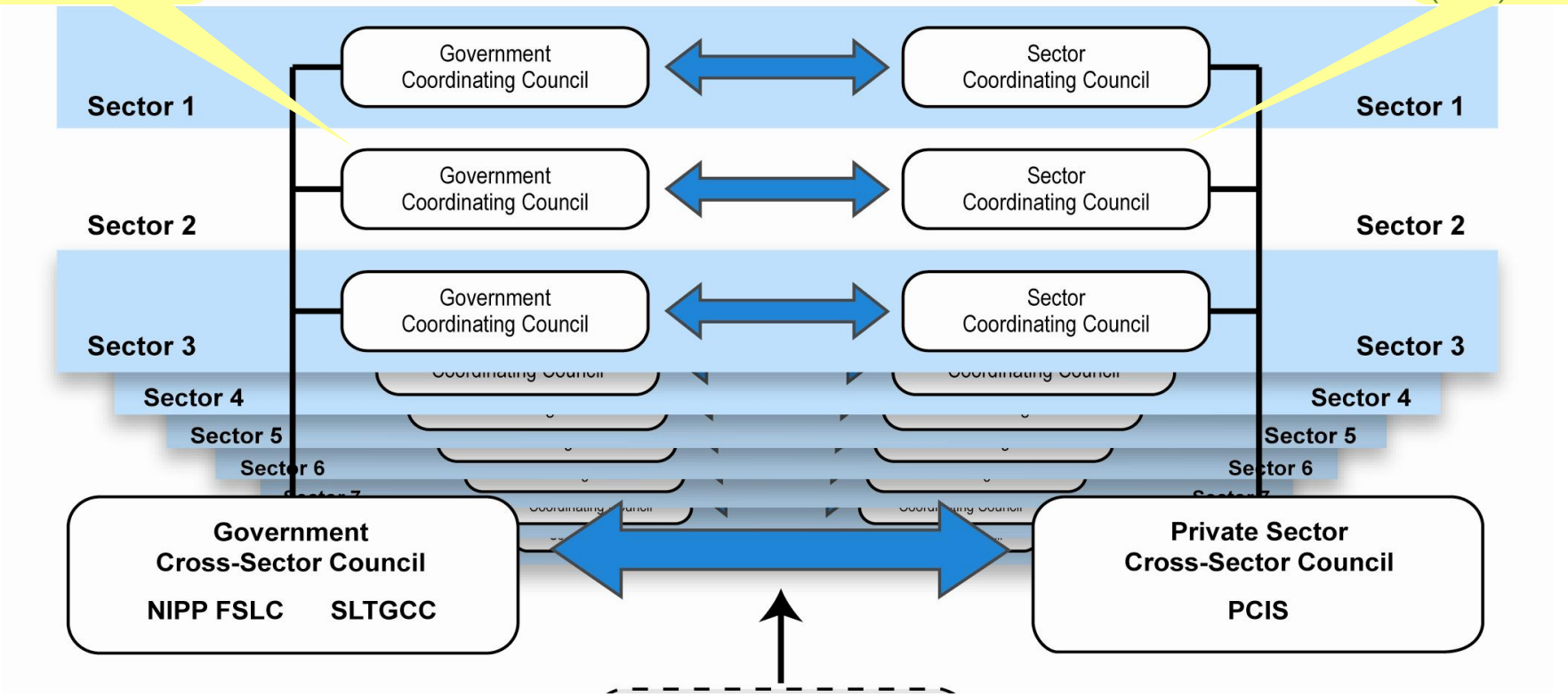


The NIPP can be accessed at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

THE NIPP SECTOR PARTNERSHIP MODEL

IT Government Coordinating Council (GCC)

IT Sector Coordinating Council (SCC)



PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY (PCIS)

The Partnership for Critical Infrastructure Security (PCIS) is a unique organization that enables owners and operators of the Nation's most critical infrastructures to collaborate on cross-sector and interdependency issues. PCIS provides a forum to build trusted and active collaboration across sectors that aim to improve emergency readiness, and build safe, secure, and resilient infrastructures.

PCIS was designated as the Private Sector Cross-Sector Council in the National Infrastructure Protection Plan (NIPP) to provide leadership on cross-sector initiatives and critical infrastructure protection preparedness and resiliency

PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY (PCIS)

Our Mission

The mission of the Partnership for Critical Infrastructure Security (PCIS) is to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services.

This mission encompasses physical, cyber, and human security that rely on strong infrastructure integrity and resilience. Accordingly, the PCIS mission spans the full spectrum of critical infrastructure matters from prevention, planning, and preparedness to business continuity, mitigation, response, and recovery. PCIS focuses primarily on cross-sector policy, strategy, and interdependency issues affecting the critical infrastructure sectors.

PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY (PCIS)

PCIS has forged responsible and productive partnerships based on these core principles:

1. Promote effective collaborative relationships between the sectors and government by improving coordination, cooperation, and communication

2. Promote a comprehensive all-hazards, all-threats approach to infrastructure protection

3. Promote the merits of a non-regulatory approach to advance the security and resilience of the sectors

PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY (PCIS)

Critical Sectors & Sub Sectors

Banking & Finance

Chemical

Commercial Facilities

Communications

Dams, Locks, & Levees

Defense Industrial Base

Emergency Services

Electricity

Oil & Natural Gas

Food & Agriculture

Government Facilities

Healthcare

Information Technology

Nuclear

Postal & Shipping

Transportation

- Highway & Motor Carrier
- Rail
- Public Transit
- Maritime
- Aviation

Water

Critical Manufacturing

PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY (PCIS)

Cross Sector Cyber Security Working Group

- President's Cyberspace Policy Review
- National Cyber Incident Response Plan

National Level Exercise Program

SLTGCC / RCCC

Pandemic Planning Report

Interdependencies Report

NICC Private Sector Seats

Playbook- SCC's, ISACs, etc

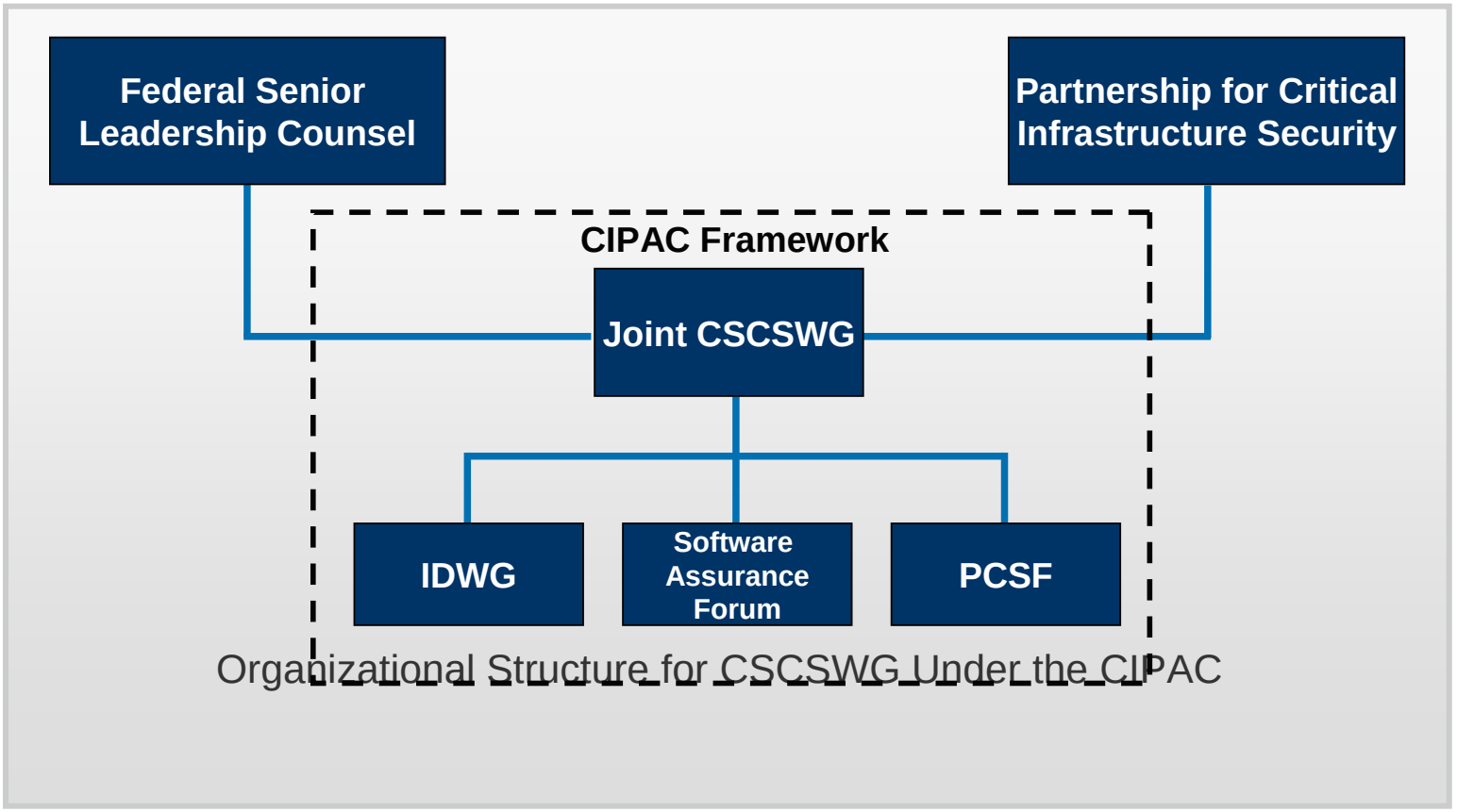
Supply Chain

Information Sharing

HSPD – 7 Rewrite

PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY (PCIS)

Cross-Sector Cyber Security Working Group



Organizational Structure for CSCSWG Under the CIPAC

NATIONAL LEVEL EXERCISE PROGRAM

TOPOFF 4 Full Scale Exercise - October, 2007

National Level Exercise 2008 - May, 2008

National Level Exercise 2009 - July, 2009

National Level Exercise 2010 - May, 2010

National Level Exercise 2011 - May, 2011

National Level Exercise 2012 -

NATIONAL LEVEL EXERCISE PROGRAM
NATIONAL PLANNING SCENARIOS

List of Scenarios

Scenario 1: Nuclear Detonation – Improvised Nuclear Device

Scenario 2: Biological Attack – Aerosol Anthrax

Scenario 3: Biological Disease Outbreak – Pandemic Influenza

Scenario 4: Biological Attack – Plague

Scenario 5: Chemical Attack – Blister Agent

Scenario 6: Chemical Attack – Toxic Industrial Chemicals

Scenario 7: Chemical Attack – Nerve Agent

Scenario 8: Chemical Attack – Chlorine Tank Explosion

Scenario 9: Natural Disaster – Major Earthquake

Scenario 10: Natural Disaster – Major Hurricane

Scenario 11: Radiological Attack – Radiological Dispersal Devices

Scenario 12: Explosives Attack – Bombing Using Improvised Explosive Device

Scenario 13: Biological Attack – Food Contamination

Scenario 14: Biological Attack – Foreign Animal Disease (Foot and Mouth Disease)

Scenario 15: Cyber Attack

Robert B. Dix, Jr.
Vice Chairman
Partnership for Critical Infrastructure Security (PCIS)

Chairman
National Private Sector Working Group
National Level Exercise 2011

Steering Group
Cross Sector Cyber Security Working Group (CSCSWG)

Vice President
Government Affairs & Critical Infrastructure Protection
Juniper Networks
rdix@juniper.net
571-203-2687