JUNIPER NETWORKS

ANSI Homeland Security Standards Panel 10th Annual Plenary Meeting

Achievements from the Past Decade & Charting the Path Forward

November 9, 2011

Arlington, Virginia

Re-Emphasizing Risk Management

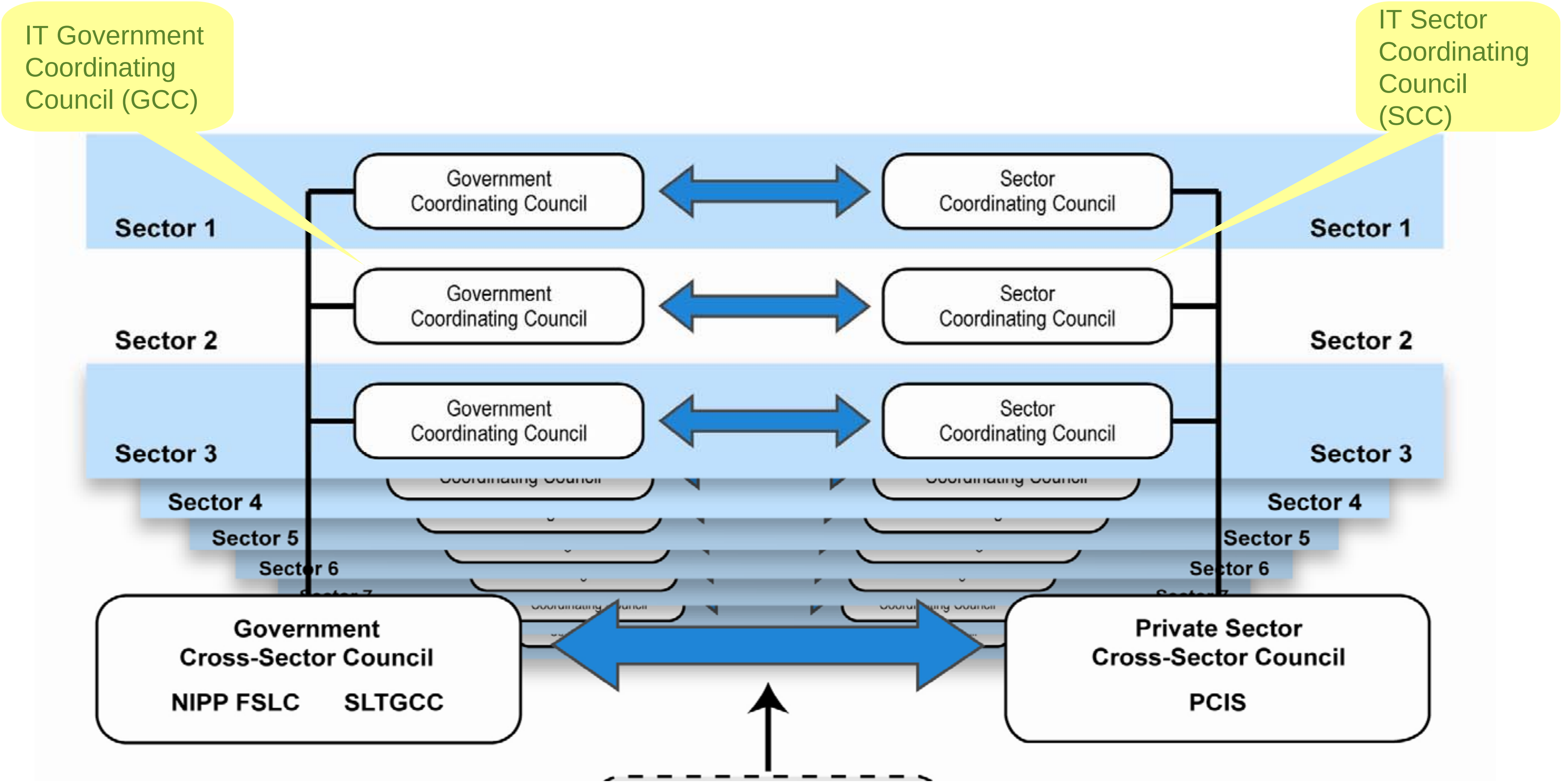
ANSI HOMELAND SECURITY STANDARDS PANEL 10TH ANNUAL PLENARY MEETING

Risk :

The potential for loss or harm due to the likelihood of an unwanted event and its adverse consequences. It is measured as the combination of the probability and consequences of an adverse event, i.e., threat. When the probability and consequences are expressed numerically, the expected risk is computed as the product of those values with uncertainty considerations….

In security, risk is based on the analysis and aggregation of three widely recognized factors: **threat, vulnerability, and consequence.**

THE NIPP SECTOR PARTNERSHIP MODEL


IT Government Coordinating Council (GCC)

IT Sector Coordinating Council (SCC)

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
Sector 4
Sector 4
Sector 5
Sector 5
Sector 6
Sector 6
Sector 7
Sector 7
Government Cross-Sector Council
NIPP FSLC
SLTGCC
Private Sector Cross-Sector Council
PCIS

NATIONAL INFRASTRUCTURE PROTECTION PLAN (NIPP)

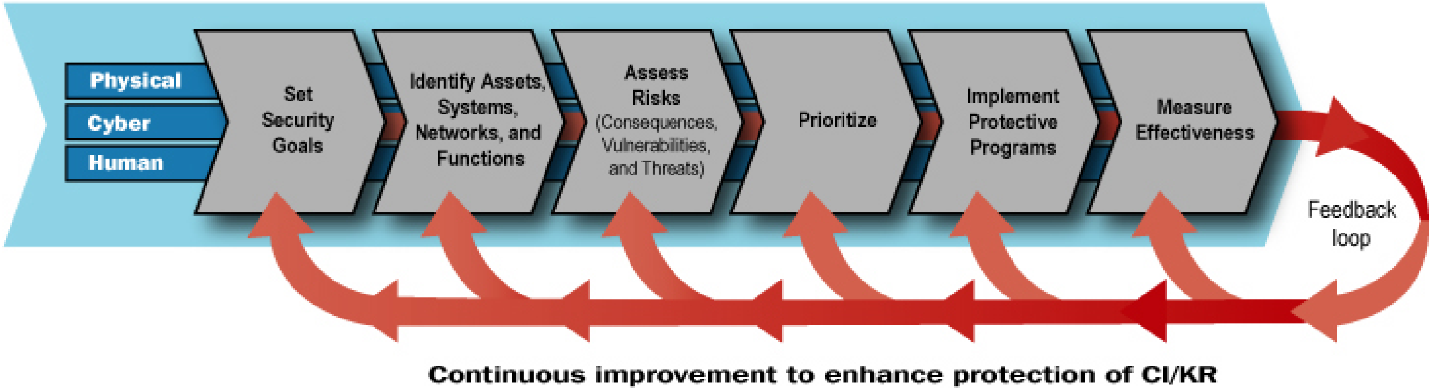
Outlines a structure for U.S. critical infrastructure protection

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

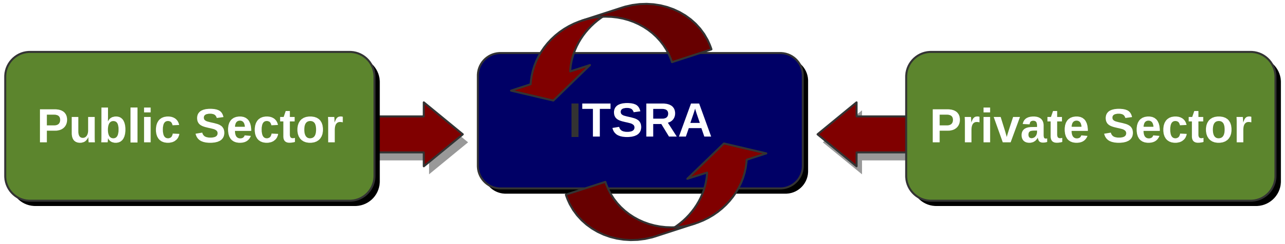
Describes responsibility to address physical, human, and cyber risk in all infrastructure sectors

NIPP Risk Management Framework


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

THE IT SECTOR BASELINE RISK ASSESSMENT (ITSRA)



The IT Sector Baseline Risk Assessment (ITSRA) is the result of unprecedented partnership among government and industry entities who engaged in a collaborative and iterative process to assess risk to critical IT Sector functions

Conducted in support of the National Infrastructure Protection Plan (NIPP)

- Sharing expertise allows for the accurate execution and refinement of the risk assessment methodology
- Sharing information enhances the prevention, protection, response, and recovery from events that impact the Sector

The IT Sector established a working group—the Risk Assessment Committee (formerly the Critical Functions and Information Sharing Working Group)—to coordinate and lead the IT Sector's risk assessment efforts

- Co-chaired by representatives of the Department of Homeland Security's National Cyber Security Division and IT Sector Coordinating Council
- Participation was conducted under the auspices of the Critical Infrastructure Protection Advisory Council (CIPAC) framework

ITSRA SCOPE: ANALYZE RISKS TO CRITICAL IT SECTOR FUNCTIONS

Focuses on Critical IT Sector Functions that are essential for national security, economic security, public health and safety, government services and the operation of other critical infrastructures

DOES NOT focus on attacks against individual networks, systems, or information theft

All-hazards risk assessment that provides an evaluation of IT Sector threats, vulnerabilities, and consequences and informs the development of strategies to mitigate sector-wide risks

An initial baseline that provides the foundation for future enhancements

The critical IT Sector functions are:

- Produce and provide IT products and services
- Provide incident management capabilities
- Provide domain name resolution services
- Provide identity management and associated trust support services;
- Provide Internet-based content, information, and communications services
- Provide Internet routing, access, and connection services

ANSI HOMELAND SECURITY STANDARDS PANEL 10TH ANNUAL PLENARY MEETING

March 30, 2011

PRESIDENTIAL POLICY DIRECTIVE/PPD-8

SUBJECT: National Preparedness

This directive is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters. Our national preparedness is the shared responsibility of all levels of government, the private and nonprofit sectors, and individual citizens. Everyone can contribute to safeguarding the Nation from harm. As such, while this directive is intended to galvanize action by the Federal Government, it is also aimed at facilitating an integrated, all-of-Nation, capabilities-based approach to preparedness.

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 - March –
June, 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

ANSI Homeland Security Standards Panel
10th Annual Plenary Meeting

Robert B. Dix, Jr.

Vice President

Government Affairs & Critical Infrastructure Protection

rdix@juniper.net

571-203-2687

everywhere