Role of Nuclear Government Coordinating Council

2009 National State Liaison Officer's Conference

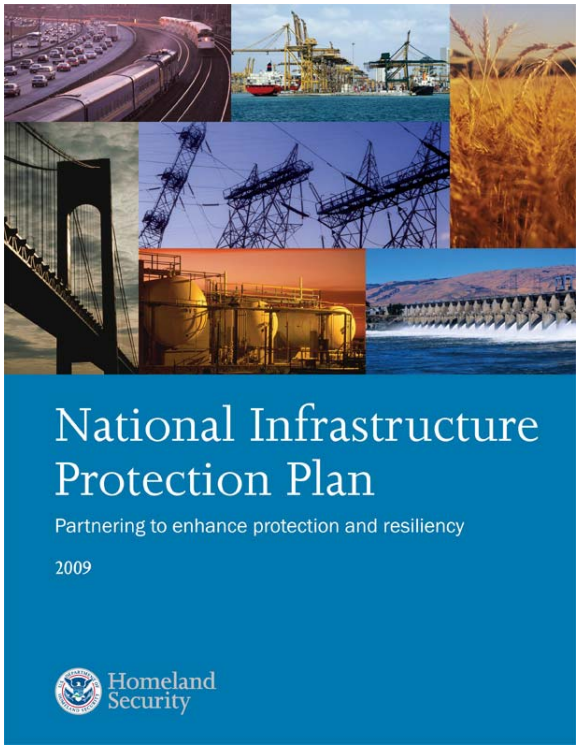
Craig Conklin, Director
Sector Specific Agency Executive Management Office

Office of Infrastructure Protection

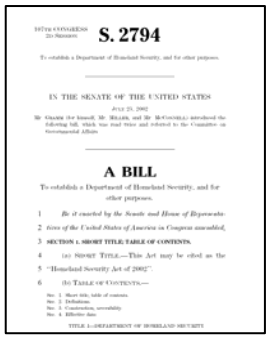
August 18, 2009

National Infrastructure Protection Plan (NIPP)

- A comprehensive plan and unifying structure for the government and the private sector to improve protection and resiliency of critical infrastructure and key resources (CIKR), including
  - Partnership model & information sharing
  - Roles & responsibilities
  - Risk management framework
  - Authorities
  - Integration with other plans
  - Building a long-term program
  - Providing resources & prioritizing investments
- Contributes to both steady-state (non-incident) risk management and incident management
- Drives IP's programs & activities, guides those of
  - Other Federal agencies and departments
  - State, local, tribal, and territorial governments
  - CIKR owners and operators



Strategic Drivers


S. 2794

IN THE SENATE OF THE UNITED STATES

A BILL

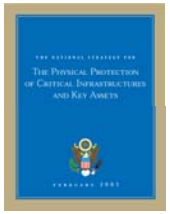
To establish a Department of Homeland Security, and for other purposes.

The Homeland Security Act of 2002 established an Assistant Secretary for Infrastructure Protection, responsible for assessing vulnerabilities of key resources and critical infrastructures and developing a comprehensive national plan. In 2006, P.L. 109-295, Section 550 directed the regulation of high risk chemical facilities.

Department of Homeland Security Appropriations Act of 2007

The DHS Appropriations Act of 2007 charged IP with creating a chemical security regulatory program. The Appropriations Act of 2008 also requires Ammonium Nitrate regulations.

The 2005 / 08 hurricanes affirmed IP's important mission and central role in preparedness.



National strategies for Homeland Security, Cyber Security, and Physical Protection of CIKR provided high-level goals and priorities for the Office of Infrastructure Protection.

HSPD-5

HSPD-7

HSPD-8

HSPD-9

HSPD-19

HSPDs provide inter-related and focused policy guidance in the areas of incident management, critical infrastructure protection, and national preparedness.

HSPD-7: drives the NIPP

HSPD-19: drives the Office of Bombing Prevention's activities

STAKEHOLDER INTERACTION

National Infrastructure Protection Plan

Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.

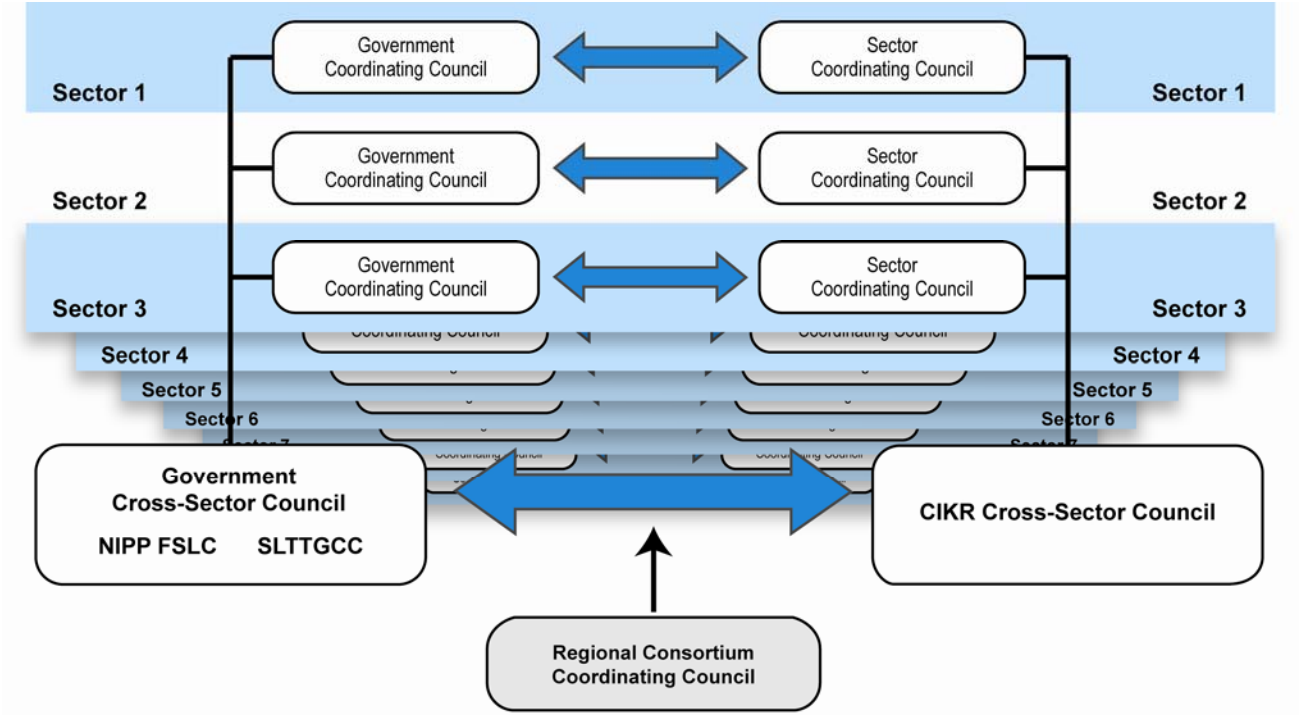
Designated Sectors & Lead Agencies from HSPD-7

- DHS coordinates the overall national effort to enhance CIKR protection and resiliency through the implementation of the NIPP
- Sector-specific agencies lead the activities in each of 18 sectors and develop and implement Sector-Specific Plans
- DHS leads 11 of the sectors
- IP leads six of these sectors

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration *United States Coast Guard*	Transportation Systems
Immigration and Customs Enforcement, *Federal Protective Service*	Government Facilities

Sector Partnership Model

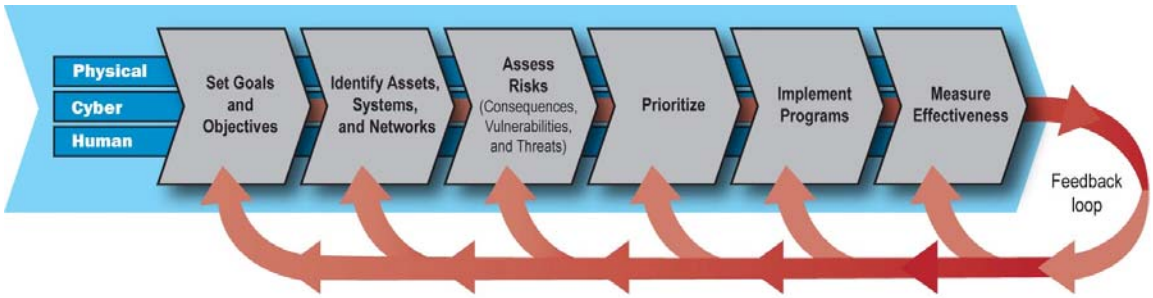
- Critical infrastructure protection and resiliency are the shared responsibilities of Federal, State, local, tribal, and territorial governments, regional coalitions, and the owners and operators of the Nation's CIKR
- NIPP outlines their roles & responsibilities
- Also describes the information-sharing environment and communications



Council functions include comprehensive planning, methodology development, risk assessment, protective programs & resiliency strategies, incident management, training, exercises, identification of R&D requirements

Risk Management Framework

- The NIPP describes processes to:
  - Set Goals and Objectives
  - Identify Assets, Systems, and Networks
  - Assess Risk (Consequences, Vulnerabilities, and Threats)
  - Prioritize
  - Implement Protective Programs & Resiliency Strategies
  - Measure Effectiveness
- IP develops methodologies with and for its partners for risk assessment, risk prioritization, and performance measurement
- The Sector-Specific Plans tailor these processes for each sector and describe sector-specific approaches and methodologies



Continuous improvement to enhance protection of CIKR

Sector-Specific Plans (SSPs)

- Tailor application of the NIPP risk management framework to each of the CIKR sectors
- Address the unique characteristics and risk landscapes of each sector
- Sector-Specific Agencies partnered with Sector Coordinating Councils and Government Coordinating Councils to develop the SSPs
- SSPs were released in May 2007 and underwent annual review in 2008
- SSPs will undergo a triennial review for reissue in 2010

Sector Specific Agency (SSA)

Primary SSA responsibilities include:

- Implementing the NIPP sector partnership model and risk management framework.
- Developing and updating the Sector Specific Plan.
- Assessing sector-level performance to enable protection-program gap assessment.
- Identifying protection priorities.
- Coordinating and supporting risk assessment & management programs for high-risk CIKR.
- Developing Sector Annual Report on efforts to identify, prioritize, and coordinate CIKR protection.
- Providing sector-specific CIKR information for incident response

Nuclear Sector Overview

- Nuclear Power Plants – 104 power reactors at 65 sites
- Research and Test Reactors – 33 reactors in 23 states
- Radioisotopes – portable sources primarily for medical and industrial use
- Other nuclear significant facilities:
  - 28 irradiation facilities
  - 12 major manufacturers/distributors of radioactive sources
  - 8 major fuel fabrication and production facilities
  - 6 spent fuel storage facilities
  - 4 mixed waste facilities
  - 1 uranium hexafluoride production facility

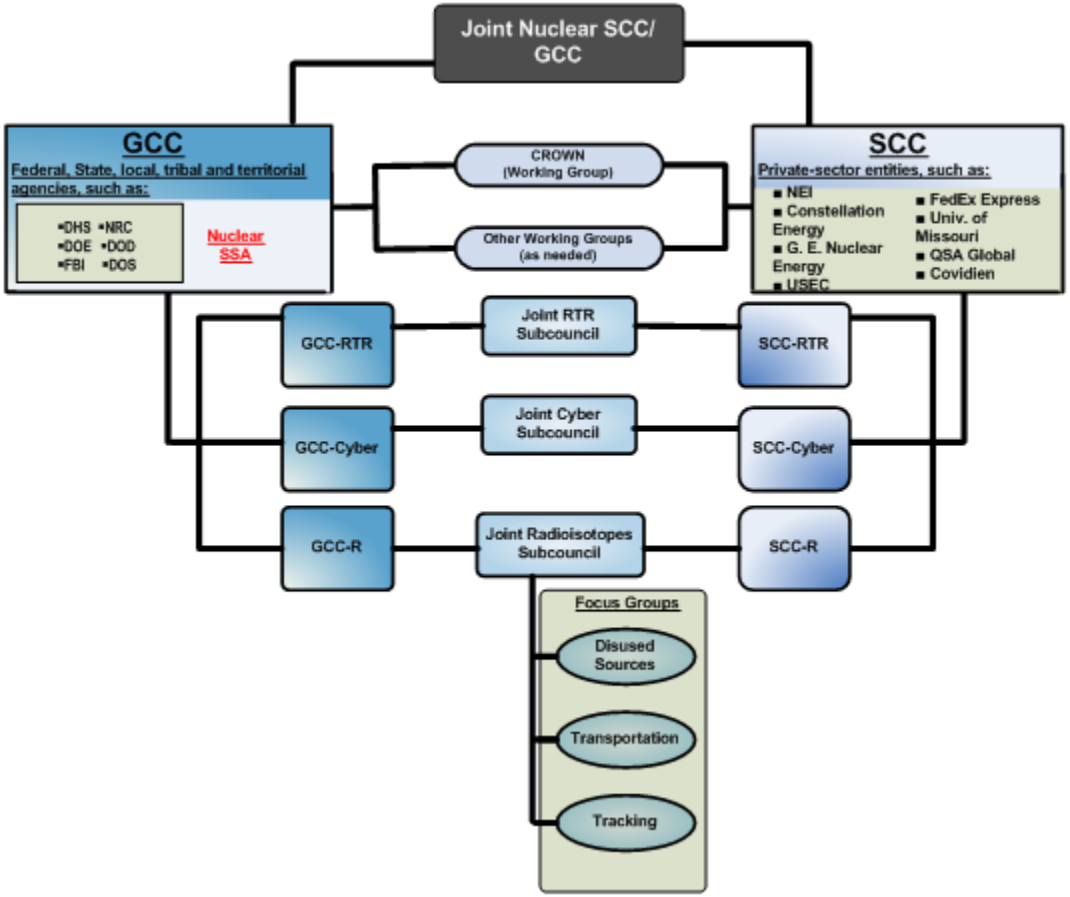
Nuclear Sector Goals

The Nuclear SCC and GCC agreed on eight security goals for the partnership to pursue above and beyond existing regulation.	
Awareness	
Goal 1	Establish permanent and robust collaboration and communication among all stakeholders having security and emergency response responsibilities for the Nuclear Sector.
Goal 2	Obtain information related to other CI/KR assets' dependencies and interdependencies with the Nuclear Sector and share it with sector security partners.
Goal 3	Increase public awareness of sector protective measures, consequences, and proper actions following a release of radioactive material.
Prevention	
Goal 4	Improve security, tracking, and detection of nuclear and radioactive material in order to prevent it from being used for malevolent purposes.
Goal 5	Coordinate with Federal, State, and local law enforcement agencies to develop protective measures and tactics to deter, detect, and prevent terrorist attacks on nuclear facilities and other Nuclear Sector assets.

Nuclear Sector Goals (continued)

Protection, Response, and Recovery	
Goal 6	Protect against exploitation of the Nuclear Sector's cyber assets, systems, networks, and the functions they support.
Goal 7	Use a risk-informed approach that includes security considerations to make budgeting, funding, and grant decisions on all identified potential protection and emergency response enhancements.
Goal 8	Enhance the ability of Federal, State, Territorial, local, and tribal governments, and the private sector to effectively respond to nuclear and radiological emergencies that result from terrorist attacks, natural disasters, or other incidents.

Nuclear CIPAC Structure



Objectives of the Nuclear GCC

- Work with public and private partners to coordinate and implement civilian nuclear security strategies, activities, and policies
- Facilitate effective communications across the government and between the government and the private sector to support the Nation's nuclear homeland security mission
- Coordinate with the existing emergency management and public health and safety communities regarding response and recovery issues associated with a terrorist act

Membership of the Nuclear GCC

- Department of Homeland Security (Chair)
- Nuclear Regulatory Commission
- Federal Bureau of Investigation
- Department of Energy
- Department of State
- Department of Transportation
- Environmental Protection Agency
- State Radiation Control Program Directors

Objectives of the Nuclear SCC

- Provide a mechanism through which the nuclear industry may provide input into nuclear CIKR protection policy development and implementation
- Provide a forum for companies and key organizations involved in nuclear security issues to cooperate with government on nuclear CIKR protection
- To achieve these objectives, the Nuclear SCC will generally consist of:
  - Six members from companies owning or operating at least one commercial nuclear power reactor
  - One member from the owners of fuel manufacturing or fuel fabrication facilities
  - One member from the manufacturers of nuclear reactors or components
  - Two members from the National Organization of Test, Research, and Training Reactors (TRTR)
  - One member from a nuclear waste management or transportation company
  - One member from the Nuclear Energy Institute

Comprehensive Reviews (CRs)

- Federal, State, local government, and private sector participation
- Conducted at all 65 nuclear power plants
- Identified potential security enhancements beyond regulatory requirements
- Final Integrated Protective Measures Analysis (IPMA) Report issued in March 2008

Comprehensive Reviews Outcome Working Network (CROWN)

- Created as a public-private working group of the NSCC-NGCC
- Obtain information on status of potential enhancements identified in the CRs and to facilitate implementation when possible
- Interagency effort includes DHS, FBI, USCG, NRC, Organization of Agreement States, and the private sector

Current Crown Enhancement Status Update (as of July 23, 2009)

	Implemented	In the Process of being Implemented	Planned to be Implemented	Not Necessary to Implement	Unable to Status	Not Yet Fully Evaluated	Total
SSA	326	165	56	223	119	225	1114
FBI	47	30	19	14	0	258	368
NSCC	61	21	17	83	0	22	204
USCG	34	19	29	27	0	14	123
Total	468	235	121	347	119	519	1809

Integrated Pilot Comprehensive Exercise (IPCE)

- Purpose
  - Ensure State, local, and Federal tactical response to a security incident is properly coordinated
  - Evaluate the relevant Tactical Take-back Tool (TTT)
  - Serve as framework for future exercises with the same goal
  - Implement potential enhancements identified in CRs

- December 13, 2008 pilot at Limerick Generating Station, with participation from:
  - Federal (FBI, DHS, NRC, FEMA)
  - State and local (Pennsylvania State Police, Chester-Montgomery County Emergency Response Team, Limerick Township Police)
  - Private sector (Exelon, NEI)

IPCE Positive Lessons-Learned

- **Integrated and coordinated response**
  - Proper coordination between agencies prevented friendly fire
  - The integration of the federal, local, and LGS personnel was seamless, thorough and efficient
- **Application of the National Incident Management System and Incident Command System**
  - Proper ICS system in place - no conflicts in authority
  - Casualty handling plan and incident command system form with medical plan was completed prior to exercise
- **Application of the Tactical Take-back Tool**
  - All teams had the tool and made use of it
  - Operators pulled up the information they needed when they needed it
  - The exercise provided a great opportunity for teams to familiarize themselves with the tool

IPCE Areas for Improvement

- **Uniformity of group tactics**
  - There was some confusion with casualty handling during the first iteration
  - Too many people were trying to talk on the radio at once during the first iteration
- **Degraded technical communications**
  - There were technical issues with the radios - concrete structure/wattage parameters.
  - There were issues with the patch system between transmissions (e.g. no priority and step-ons) and the team was forced to utilize CAS in order to establish command priority on the radio
- **Further R&D to refine the Tactical Take-back Tool**
  - There is a need for periodic updates of the TTT to accommodate modifications to plant which would normally be expected to occur over time
  - Power point projectors and laptops should be part of the Take-back Tactical Tool and made available to the SWAT team leaders to expedite their briefings and facilitate more effective screen display

Radioactive Materials – Focus Groups

- Removal and Disposition of Disused Sources
  - Develop clear, concise, single message on potential national security concerns presented by lack of commercial disposition options for sealed sources

- Radioactive Materials Tracking
  - Identify existing commercially available tracking technologies and evaluate their ability of to track conveyances, packages, and sources

- Transportation of Radioactive Materials
  - Identify and address potential national security concerns associated with transportation and transshipment of radioactive materials

Research & Test Reactor (RTR) Voluntary Security Enhancement Program

- DHS, DOE, NRC and RTR community participation
- Successful pilot conducted at two sites (University of Missouri-Columbia and Oregon State)
- Endorsed by NSCC and Test, Research and Training Reactor (TRTR) Organizations
- As of July 2009, nine reactors out of 34 eligible have volunteered for voluntary enhancements

Blood Irradiator In-Device Delay (IDD) Program

- Significantly increase time needed for unauthorized source removal
- Scope includes 843 of estimated 1,000 cesium irradiators in U.S.
- NNSA oversees IDD effort for all three major irradiator manufacturers:
- Endorsed by OAS, NRC, NNSA, and DHS
- National Implementation underway
  - New devices to have IDD preinstalled
  - Installations for existing devices projected through 2016
  - As of June 2009, 25 kits have been installed

Sector Specific Agency Executive Management Office Contact Information

- ***Craig Conklin, Craig.Conklin@hq.dhs.gov, (703) 235-2850***
- ***Marc Brooks, Marc.Brooks@hq.dhs.gov, (703) 235-3970***

or

- NuclearSSA@hq.dhs.gov

Homeland Security