The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Nuclear Sector Collaboration, Information Sharing, and Joint Cyber Subcouncil Overview

March, 2018

Homeland Security

Sector Outreach and Programs Division

Primary Focus:

- Build, align and leverage national public-private partnerships and programs to enhance critical infrastructure security and resilience.

How do we accomplish our mission?

- Partnership Collaboration Structures
- Sector-Specific Agency Management Responsibilities
- Sector-Specific and Cross-Sector Programs and Resources

Partnership and Collaboration Structures

Sector and cross-sector structures include:

- Sector Coordinating Councils
- Critical Infrastructure Cross-Sector Council
- Government Coordinating Councils
- Federal Senior Leadership Council
- State ,Local, Tribal, and Territorial Government Coordinating Council
- Regional Consortium Coordinating Council
- Information Sharing Organizations

Partnership and Collaboration Structures (cont.)

SOPD provides operational oversight & administrative support to the Critical Infrastructure Partnership Advisory Council (CIPAC).

- DHS established CIPAC in 2006 under the authority of the Homeland Security Act of 2002, as a partnership framework exempt from the Federal Advisory Committee Act (FACA).
- CIPAC enables private sector and government stakeholders to work in partnership and meet during joint Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) meetings.
- CIPAC provides the legal framework from cross-sector collaboration.

Homeland Security

Nuclear Sector Specific Agency (SSA)

Under the NIPP and PPD-21, the SSA's responsibilities include:

- Coordination of risk management activities to improve the protection and resilience of the Nuclear Sector beyond what is required by regulation.
- Development, in coordination with sector partners, of the Nuclear Sector-Specific Plan (SSP) and SSP updates.
- Identification and prioritization of Nuclear Sector risk management activities, in coordination with sector partners, as reported in the Nuclear Sector Annual Report (SAR).
- Assessment of Nuclear Sector protection and resilience program performance.
- Provision of sector-specific information, as appropriate, to support incident management activities.

Homeland Security

Nuclear Sector Joint Cyber Subcouncil

The Nuclear Sector Joint Cyber Subcouncil convenes quarterly to develop and recommend policies, strategies, plans and measures that will enhance the cyber security of the nation's Nuclear Sector under the auspices of the National Infrastructure Protection Plan (NIPP) and the Critical Infrastructure Protection Advisory Council (CIPAC).

Homeland Security

Joint Cyber Subcouncil - Membership

Subcouncil Membership include:

- Nuclear Sector Coordination Council-Cyber (NSCC-Cyber)
- Nuclear Sector-Specific Agency (SSA)
- Nuclear Regulatory Commission (NRC)
- Department of Energy (DOE)
- Federal Bureau of Investigation (FBI)
- DHS Intelligence & Analysis (I&A)
- DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- DHS Office of Cybersecurity & Communication (CS&C)

Homeland Security

8

Joint Cyber Subcouncil - Objectives

- Improve cybersecurity knowledge, tools, capabilities, and practices across the sector
- Facilitate dialogue between private sector partners, Federal regulators, other Federal cybersecurity officials, and the intelligence community
- Identify and assess sector-specific cyber threats, risks, vulnerabilities, and consequences.
- Develop programs and measures that cost-effectively reduce cyber risks from all-hazard incidents.
- Support planning and risk mitigation that enables coordinated response and rapid recovery following cyber incidents.
- Promote continuous learning and adaptation among partners.

Homeland Security

10

Key Cyber Considerations for the Nuclear Sector

- Physical systems at existing facilities are increasingly being reconfigured to link with cyber networks, creating potential vulnerabilities.
- Recent targeting of digital systems including corporate networks or SCADA systems through malware or ransomware attacks.
- Adversaries may attempt blended cyber and physical attack methods to achieve desired results
- Increasing potential for cybersecurity risks related to Unmanned Aerial Systems (UAS).

Homeland Security

9

Joint Cyber Subcouncil – Activities

- Coordination with CS&C-led initiatives such as Automated Indicator Sharing and the Industrial Control Systems Joint Working Group (ICSJWG).
- Participate in sector-specific and cross-sector exercises testing cyber coordination and information sharing.
- Hold periodic or ad-hoc teleconference briefings to address emergent cyber threats and vulnerabilities impacting the nuclear sector.
- Update and communicate plans and strategies like the Roadmap to Enhance Cyber Systems in the Nuclear Sector and NIST Cybersecurity Framework

Homeland Security

12

Additional Nuclear SSA Cyber Activities

- Quarterly Joint Nuclear CIPAC Meeting Provide a forum where the NGCC and NSCC can share information, coordinate strategies, activities and policies as it relates to cyber security concerns of the sector.
- Quarterly Classified threat briefings address both cyber and physical security concerns relevant to the nuclear sector.
- Nuclear Sector Intelligence Working Group will establish mechanisms for gathering and sharing intelligence related to cyber incidents, risks, threats, and vulnerabilities impacting the sector.

Homeland Security

15

Homeland Security