Critical Infrastructure Partnership Overview

Chris Boyer
AVP – Global Public Policy
December 11, 2017
The U.S. government defines critical infrastructure as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof."
The U.S. government requires private industry in each critical economic sector to:

- Assess vulnerabilities - both physical or cyber
- Plan to eliminate significant vulnerabilities;
- Develop systems to identify and prevent attempted attacks;
- Alert, contain and rebuff attacks and then, with the Federal Emergency Management Agency (FEMA) to rebuild essential capabilities.

**Sector Coordinating Councils ("SCCs")** Conducts planning activities with government on behalf of industry. Includes the following:

- Coordination between critical infrastructure owners, operators and suppliers;
- Supporting information sharing capabilities,
- Providing input on R&D,
- Developing industry standards and practices.
Critical Infrastructure Partnership Advisory Council (CIPAC)

Roles and Responsibilities – Government

• **Government Coordinating Council** - government counterpart for each Sector Coordinating Council (SCC).

• **Sector Specific Agency (SSA)** – Each sector of critical infrastructure has a corresponding SSA that facilitates the GCC and coordinates activities with the sector.

• **Information Sharing** – DHS has multiple programs to share information with industry:
  
  • National Cybersecurity and Communications Integration Center (NCCIC),
  
  • Automated Indicator Sharing (AIS) program,
  
  • Cybersecurity Information Sharing and Collaboration Program (CISCP)

• **Prioritized Restoration** – Priority access during disaster recovery incidents

• **Critical Infrastructure Vulnerability Assessments** – Optional field assessments to identify vulnerabilities, interdependencies, capabilities etc.
Communications Sector Partnership with Government

National Security Telecommunications Advisory Committee (NSTAC) – Policy
- Established in 1982
- Policy advise to the President
- Recent reports – botnet mitigation, emerging technologies strategic vision, big data analytics and national security etc.

National Cybersecurity & Communications Integration Center (NCCIC) – Operations
- On call 24/7 center
- Comms ISAC
- US CERT
- ICS CERT
- National Coordinating Center (NCC)

Communications Sector Coordinating Council (CSCC) – Planning
- Established in 2006
- Executive Order Implementation
- NIST Framework
- Communications Sector Specific Plan (CSSP)
- National Incident Response Plan
- Information Sharing & Analysis Organizations