Critical Infrastructure Protection: A Primer… With a Twist

2018 SCGMIS Network and Telecom Workshop

Thursday, October 18, 2018

Presented by Lyle Hendrick

Presentation objectives:

- Explain what is Critical Infrastructure Protection (CIP)
- Identify CIP origins and history
- Increase awareness of CIP
- List Key Critical Infrastructure Sectors
- Provide resources to aid in securing your respective organization

What is Critical Infrastructure Protection?

- It is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation.

Origins and history

The U.S. CIP is a national program initiated In May 1998 when President Bill Clinton issued presidential directive PDD-63. It was updated on December 17, 2003, by President Bush through Homeland Security Presidential Directive HSPD-7.

Who is responsible?

The **Office of Infrastructure Protection (IP)** leads and coordinates national programs and policies on critical infrastructure security and resilience and has established strong partnerships across government and the private sector.

National Infrastructure Protection Plan

The **National Infrastructure Protection Plan (NIPP)** is a document called for by Homeland Security Presidential Directive 7, which aims to unify Critical Infrastructure and Key Resource (CIKR) protection efforts across the country.

Critical Infrastructure Sectors

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector (ESS)
- Energy Sector

Critical Infrastructure Sectors cont.

- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

InfraGard

InfraGard is a non-profit organization serving as a public-private partnership between U.S. businesses and the Federal Bureau of Investigation. The organization is an information sharing and analysis effort serving the interests, and combining the knowledge base of, a wide range of private sector and government members.

October is National Cybersecurity Awareness Month, commemorating its 15th year as an annual initiative to raise awareness about the importance of cybersecurity.

NCSAM General Toolkit 2018

Cybersecurity is our shared responsibility and we all must work together to improve our Nation's cybersecurity.

- "Strengthen the Nation's Cybersecurity Ecosystem"
- "Tackle it Together"
- "Build up the Cybersecurity Workforce"
- "Secure Critical Infrastructure from Cyber Threats"

References and resources

https://en.wikipedia.org/wiki/Tappan_Zee_Bridge_(2017–present)

https://en.wikipedia.org/wiki/Critical_infrastructure_protection

https://www.dhs.gov/office-infrastructure-protection

https://www.dhs.gov/sites/default/files/publications/NCSAM_GeneralToolkit_final.pdf

Contact information

Lyle Hendrick

Cell: 803 603 0203

Email: windeagle20032002@yahoo.com