U.S Election Assistance Commission

Elections as Critical Infrastructure:

Background

Purpose of Presentation

Develop a baseline understanding of Critical Infrastructure (CI)

Explain how elections fit within CI

What is Critical Infrastructure (CI)?

- **The current definition comes from The Patriot Act**
- **The Patriot Act defines "critical infrastructure" (CI) as:**
  - **systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Sec. 1016(e)).**

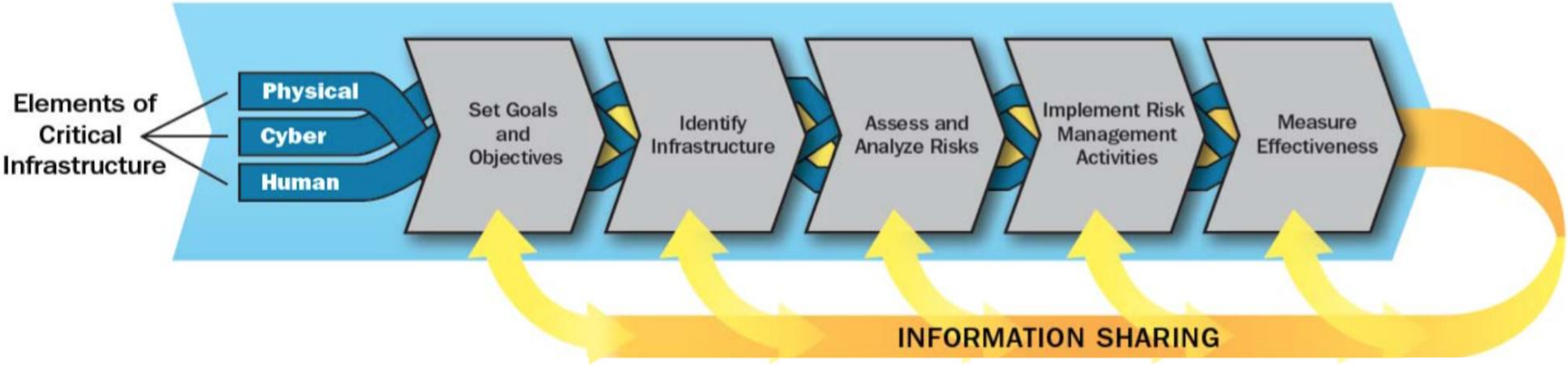
CI is a Patriot Act initiative to protect vital systems and assets

History of Critical Infrastructure

- **In response to the terror attacks of September 11, 2001, Congress passed the USA PATRIOT Act of 2001(P.L. 107-56).**
- **Purpose: To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.**
- **Justification: Private business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures.**

The current definition of CI was a response to 9/11 to protect critical assets

Goals and Framework of CI



Three strategic imperatives shall drive the Federal approach to strengthen critical infrastructure security and resilience:

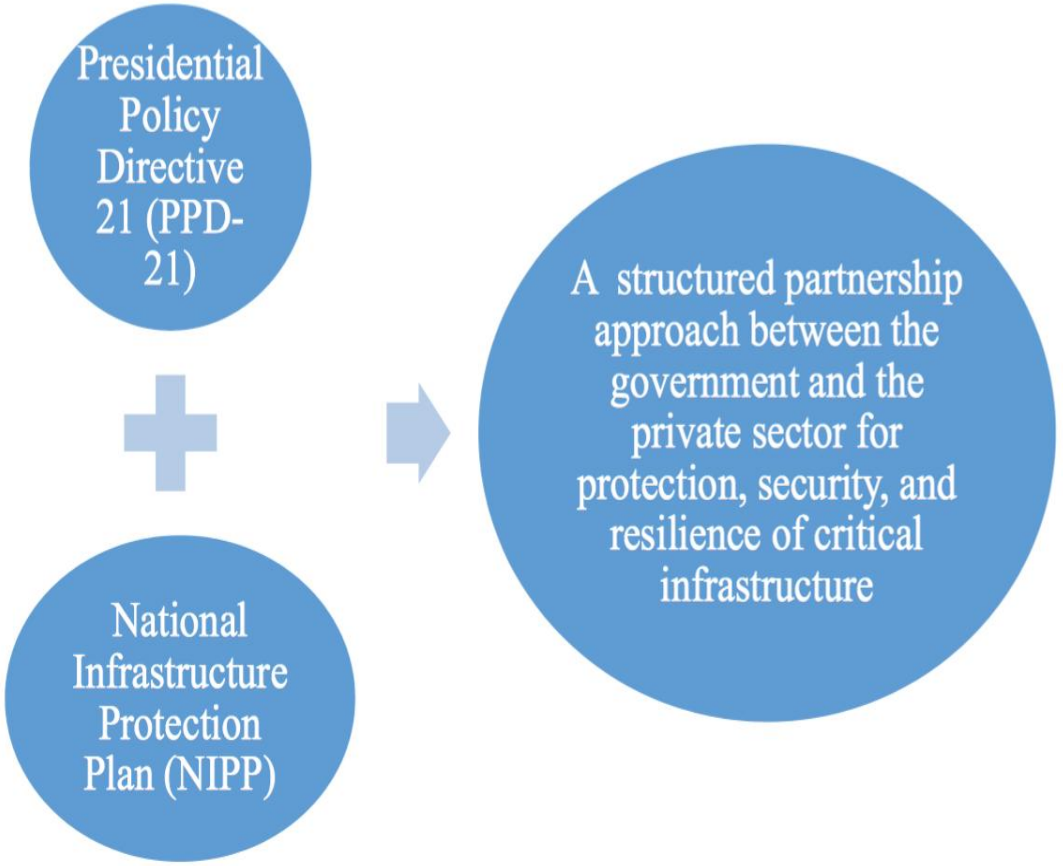
1) Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience

2) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government

3) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

Guiding Documents and Framework

These documents establish the mechanisms for collaboration between the private sector and government in protecting CI



Key Entities and Roles Within a CI Sector

- **Department of Homeland Security (DHS)** – Leads the national effort by providing strategic guidance, promoting national unity of effort, and coordinating the overall Federal effort.
- **Sector-Specific Agencies (SSAs)** – Coordinates and collaborates with DHS and other relevant Federal departments and agencies, with CI owners and operators.
- **Sector Coordinating Councils (SCCs**) – SCCs serve as principal collaboration points between the government and private sector owners and operators. They consist of representatives from the private sector.
- **Government Coordinating Councils (GCCs**) – Consist of representatives from various levels of government (including Federal and State, Local, Territorial and Tribal (SLTT)), as appropriate to the operating landscape of each individual sector.
- **State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)** –SLTTGCC promotes the engagement of SLTT partners in national critical infrastructure.

Sector-Specific Agency (SSA) Definition and Role

- **Definition:**
- Sector- a logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; the *National Plan* addresses 16 critical infrastructure sectors. Additionally, sub-sectors can be created.
- **SSA Roles:**
- Serve as a day-to-day Federal interface for the dynamic prioritization, collaboration, and coordination of sector-specific activities.
- Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations.
- Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate.
- Support the Secretary of Homeland Security's statutory reporting requirements by providing, on an annual basis, sector-specific CI information.

16 Critical Infrastructure Sectors and Their Corresponding Agencies & Councils

Critical Infrastructure Sector	Sector Specific Agency	Critical Infrastructure Partnership Advisory Council: Sector Coordinating Councils (SCCs)	Critical Infrastructure Partnership Advisory Council: Government Coordinating Councils (GCCs)	Critical Infrastructure Partnership Advisory Council: Regional Consortia
Chemical	Department of Homeland Security	✓	✓	
Commercial Facilities ⓘ	Department of Homeland Security	✓	✓	
Communications ⓘ	Department of Homeland Security	✓	✓	
Critical Manufacturing	Department of Homeland Security	✓	✓	
Dams	Department of Homeland Security	✓	✓	
Emergency Services ⓘ	Department of Homeland Security	✓	✓	
Information Technology ⓘ	Department of Homeland Security	✓	✓	
Nuclear Reactors, Materials & Waste	Department of Homeland Security	✓	✓	
Food & Agriculture	Department of Agriculture, Department of Health and Human Services	✓	✓	
Defense Industrial Base ⓘ	Department of Defense	✓	✓	
Energy ⓘ	Department of Energy	✓	✓	
Healthcare & Public Health ⓘ	Department of Health and Human Services	✓	✓	
Financial Services ⓘ	Department of the Treasury	Uses separate coordinating entity	✓	
Water & Wastewater Systems ⓘ	Environmental Protection Agency	✓	✓	
Government Facilities	Department of Homeland Security, General Services Administration	Sector does not have an SCC	✓	
Transportation Systems ⓘ	Department of Homeland Security, Department of Transportation	Various [illegible] broken down by transportation mode or subsector.	✓	

Critical Infrastructure Cross-Sector Council

Federal Senior Leadership Council

State, Local, Tribal, and Territorial Government Coordinating Council

Regional Consortium Coordinating Council

ⓘ Indicates that a sector (or a subsector within the sector) has a designated information-sharing organization.

Government Facilities Sector

- **Includes general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and other critical structures.**
- **In addition, the sector includes cyber elements that contribute to the protection of sector assets as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge.**
- **The Government Facilities Sector currently has two subsectors, Education Facilities and Monuments and Icons. Elections is the third.**

This is the CI sector in which "Elections" is designated

Education Facility Subsector (EFS)

- **The Education Department Office of Safe and Drug-Free Schools partners with DHS on this subsector.**
- **EFS has human, physical, and cyber assets. However, the EFS assets of primary concern are human and physical.**
- **The predominant characteristics of individual pre K–12 schools vary tremendously within EFS.**
- **Facilities supporting these students and staff are widely dispersed throughout the country and in all geographical regions with differing social and physical environments.**

Elections are similar to the education facility subsector (EFS)

Communications

- **Information Sharing and Analysis Centers (ISACs)**: These are "operational entities formed by CI owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders." (Source: Presidential Decision Directive 63, 1998)
- **Information Sharing and Analysis Organizations (ISAOs):** Though similar to ISACs, ISAOs are "any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of: (a) Gathering and analyzing Critical Infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof; (b) Communicating or disclosing Critical Infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to Critical Infrastructure or protected systems; and (c) Voluntarily disseminating Critical Infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (a) and (b)."
- Essentially, ISAOs allow for more widespread information sharing across sectors and among interested individuals regardless of clearance, knowledge level, or inclusion in a CI sector.

Legal Protections over Communications

- Information about security and vulnerabilities shared under the restrictions of the Critical Infrastructure Information Act is considered Protected Critical Infrastructure Information (PCII). PCII is not subject to the many disclosure regulations, such as those found in the Freedom of Information Act and its state-level counterpart. This protection, allows the critical infrastructure community to discuss vulnerabilities and problems without publically exposing potentially sensitive information.
- For those participating in election sector coordinating councils this protection means that some information communicated between DHS and the coordinating councils can be protected. This limits the potential for sensitive election security information to be made public and protects potentially sensitive material from being misconstrued or used for nefarious purposes. This protection is made possible by an exception to the Federal Advisory Committee Act created by the Critical Infrastructure Partnership Advisory Council.

Many Questions!

- The polling places themselves: Who is the first responder to polling place incidents? What happens to vote-by-mail tabulation locations? What are the procedures for privately-owned polling places (ex. churches)?
- Election Board Offices: Will election officials need to go through background checks for clearance purposes? Will this designation allow state government entities that are not election offices to alter operations of an election office? Are the office phones and networks secure? If not, what are the back ups? Are administrators and staff properly trained to handle all contingencies? Who makes this call?
- Transport and storage of ballots and voting machines: Are vendors and storage facilities secure? Who defines them as secure?

These are illustrative of the many CI questions that come with the elections designation, and must be answered as the elections subsector is implemented. The EAC is keeping an inventory of questions, and requests/welcomes election official questions at:

clearinghouse@eac.gov

The EAC's Role

The EAC has requested that DHS name the Commission as Co-SAA.

This designation is important to ensure that state and local election officials and administrators have an informed federal advocate working directly with DHS as the department determines what resources and services are needed to protect U.S. election systems and how these resources will be distributed.

The EAC has held and will continue to hold, hearings and meetings to give DHS a platform to discuss the designation and its potential benefits, as well as answer questions from stakeholders. Serving as the official Co-SSA for implementing the critical infrastructure designation would tap into this strength and provide election officials with assurance that their interests and concerns will shape the contours of DHS's plan moving forward.

DHS Contacts

- Neil Jenkins: neil.jenkins@HQ.DHS.GOV
- Geoffrey Hale: geoffrey.hale@HQ.DHS.GOV
- Robert Hanson: robert.hanson@HQ.DHS.GOV
- Juan Figueroa: juan.figueroa@HQ.DHS.GOV
- Robert Gatlin: robert.gatlin@HQ.DHS.GOV

More information at the EAC Website: www.eac.gov

- Whitepaper:
- **STARTING POINT: U.S. Election Systems as Critical Infrastructure**
- What we know:
- **Statement on the Designation of Election Infrastructure as a Critical infrastructure Subsector**
- **DHS JEOLC Presentation** (PDF)
- **Critical Infrastructure Overview Presentation** (PDF)
- **Critical Infrastructure Questions** (PDF)
- Questions from state and local officials:
- **Operational | Structural | Technical**

U.S Election Assistance Commission

Contact Information:

Christy McCormick, Commissioner

cmccormick@eac.gov

(301) 563-3965

General EAC Number: (301) 563-3939