The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Department of Homeland Security Assessing Secure and Resilient Time

WSTS Workshop

June 20, 2018

Homeland Security

Outline

- DHS Role in Critical Infrastructure
- Timing in Critical Infrastructure
- Managing Risk
  - Holistic view of risk management
  - National Infrastructure Protection Plan (NIPP)
  - National Mitigation Framework
- Notional PNT architecture (FRP)
- Way ahead

DHS is The Federal Coordinator for U.S. Critical Infrastructure

- Leads the national effort to mitigate risks to, strengthen the security of, and enhance the all-hazard resilience of critical infrastructure.
- Partners across the critical infrastructure domain, leads related preparedness activities, and serves as an information-sharing conduit between the private sector and public entities.

Security: *Reducing the risk to physical and cyber critical infrastructure caused by natural and manmade threats.*

Resilience: *The ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions.*

Homeland Security

IP is the Federal Coordinator for U.S. Critical Infrastructure

Critical infrastructure: the systems, assets, and networks that maintain our way of life. It is diverse and complex, includes varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both physical and cyber space, and governance constructs that involve multi-level authorities, responsibilities, and regulations.

Courtesy of DHS

Critical Infrastructure Defined: "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, national public health or safety, or any combination thereof."

Homeland Security

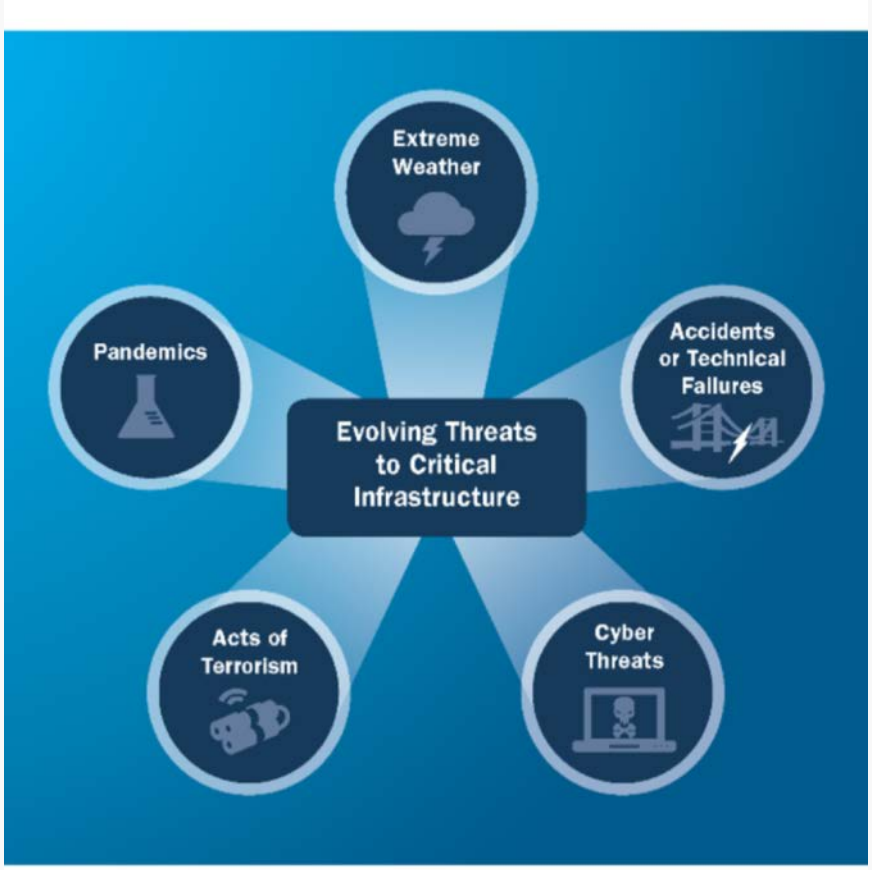
IP is the Federal Coordinator for U.S. Critical Infrastructure

Critical infrastructure: the systems, assets, and networks that maintain our way of life. It is diverse and complex, includes varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both physical and cyber space, and governance constructs that involve multi-level authorities, responsibilities, and regulations.

Time/UTC

Do you need UTC? If yes, how do you get it? How do you operate without it?

Strategies for Managing PNT Risk

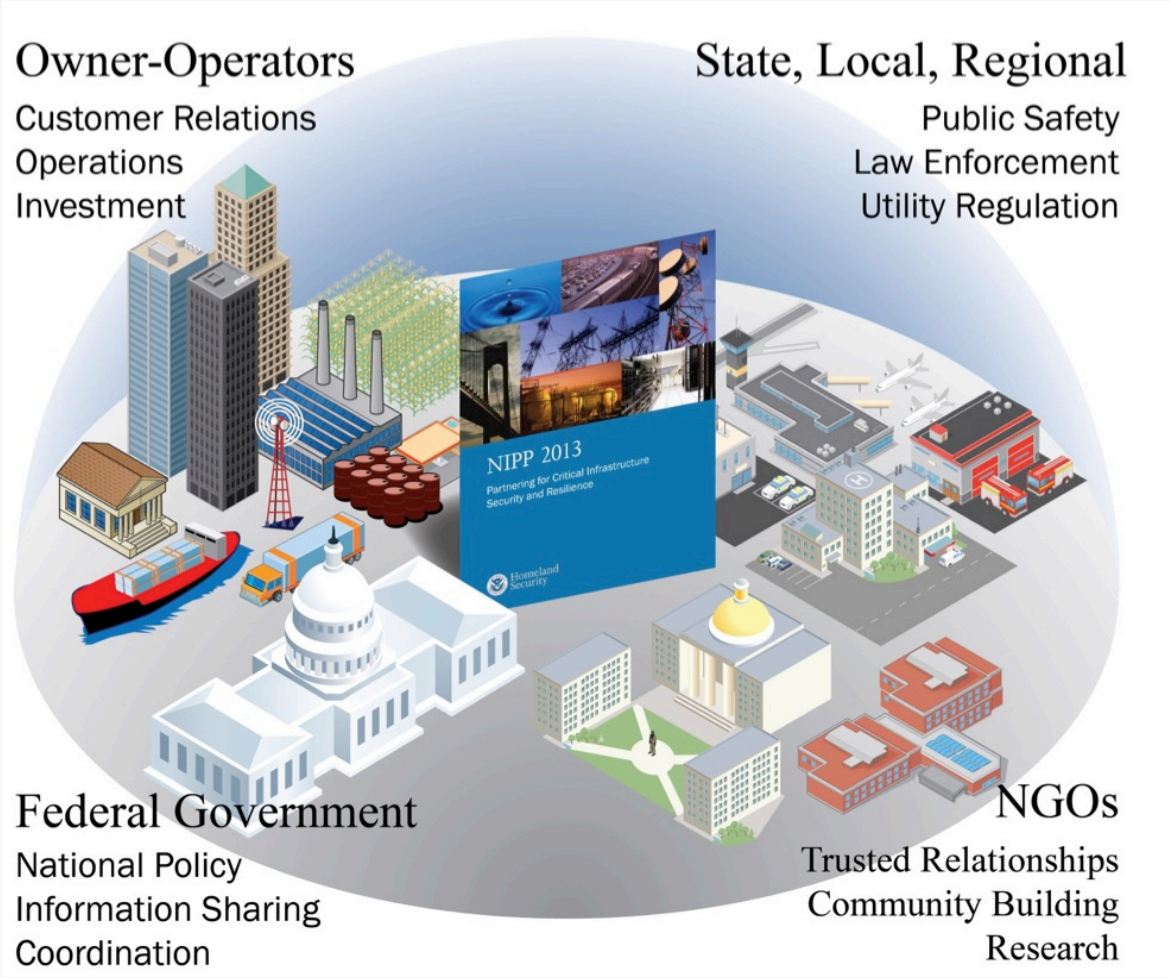


Courtesy of DHS

- Employing an integrated approach to address diverse and evolving risks
- Understanding vulnerabilities to manage GPS risks
- Educating Partners and Changing Perspectives (*e.g.*, GPS as a computer, not a radio)
- Exploring new technologies
- Keeping National Policies Relevant

Strengthening Critical Infrastructure Security and Resilience Requires Engagement with a Broad and Diverse Community of Partners

- Engaging in collaborative processes
- Applying individual expertise
- Bringing resources to bear
- Building the collective effort
- Enhancing overall effectiveness (not just timing)

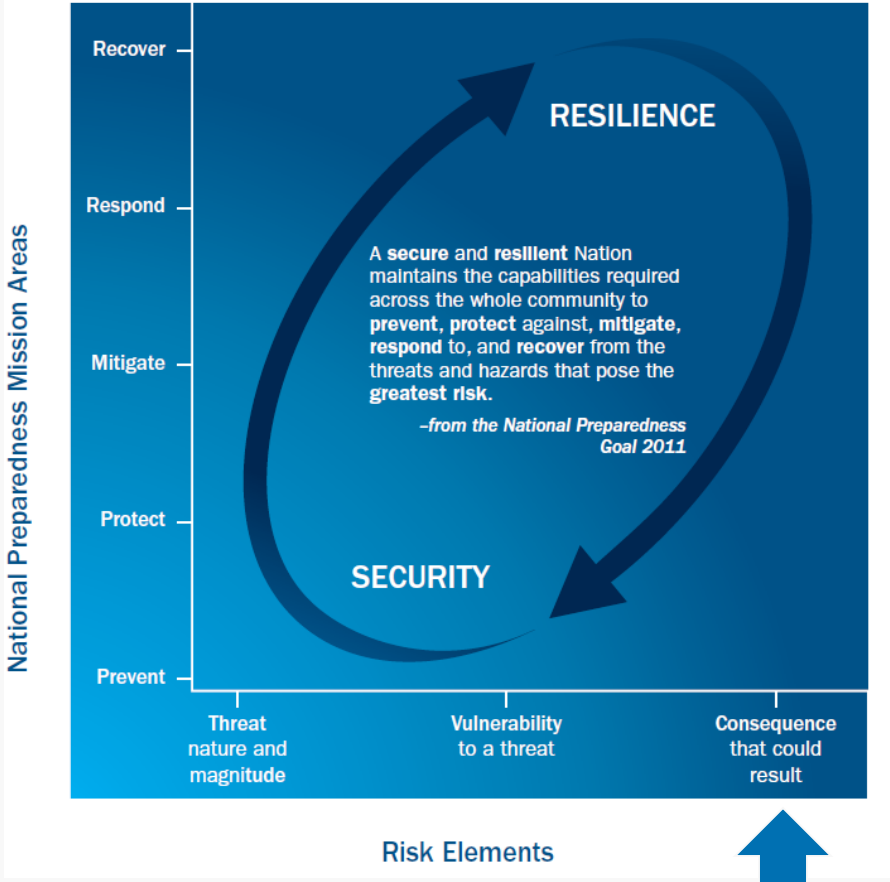


Homeland Security

National Infrastructure Protection Plan
Mitigating Consequences

- Information sharing
- Restore Critical Infrastructure, especially lifeline sectors
- Ensure that redundant processes are implemented for key functions, reducing the potential consequences
- Remove key operational functions from the Internet-connected business network
- Repair or replace damaged infrastructure with cost-effective designs that are more secure and resilient
- Utilize and ensure the reliability of emergency communications capabilities.

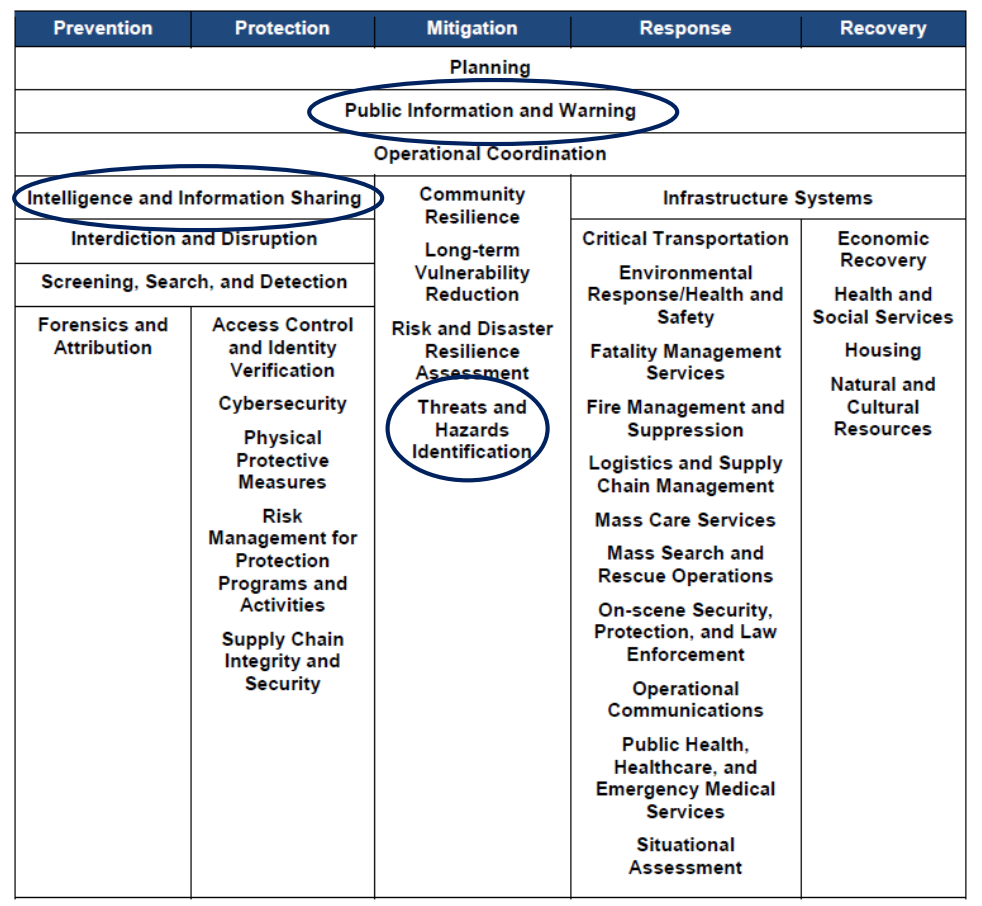
Figure 4 – Critical Infrastructure Risk in the Context of National Preparedness



The National Mitigation Framework

PNT Mitigation

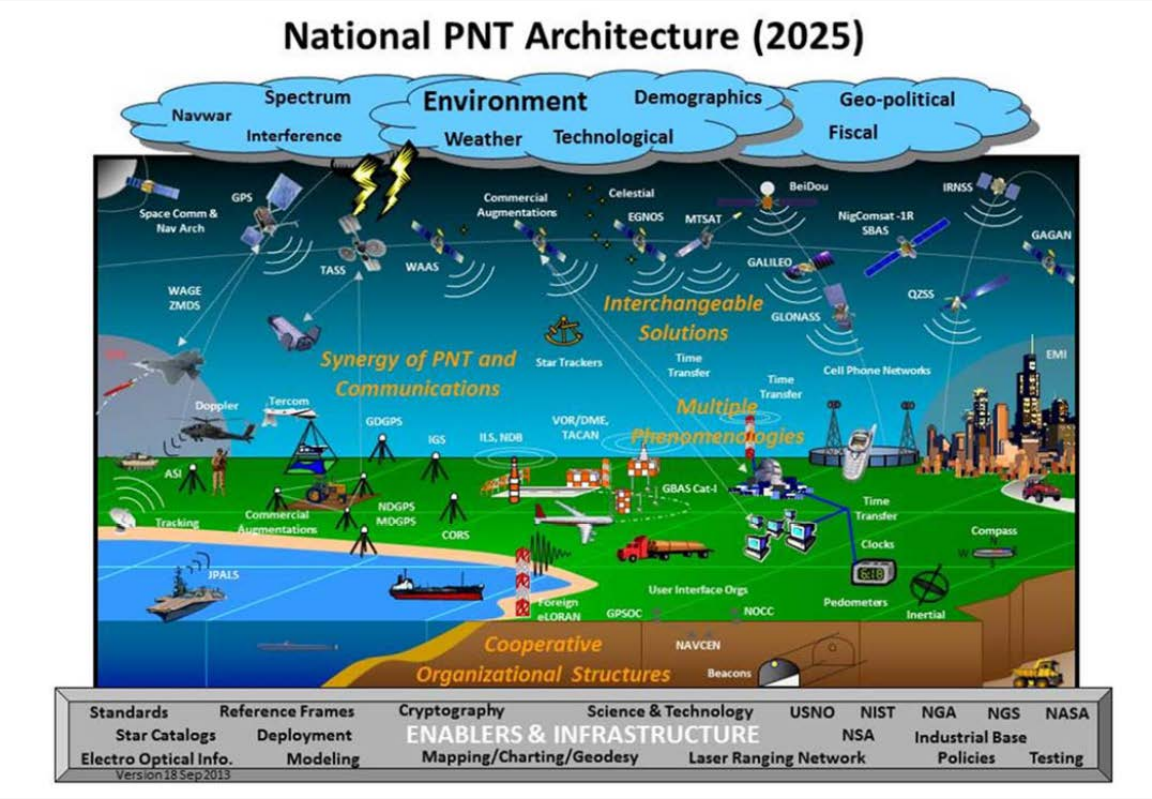
- Focus has been on Prevention and Protection
- Mitigation Efforts less energetic – more difficult
- How do we respond and recover?
- Do we understand where we fit in community efforts?
- When should we start thinking about mitigation (Hint: Design Phase)



Federal Radionavigation Plan

PNT Architecture

- Multiple Phenomenologies
- Not centrally funded
- Industry filling gaps
- Assessing alternative federal systems



Do you have a strategy to identify timing needs and select the appropriate timing sources?

Looking Forward

- Validation of Critical Infrastructure PNT requirements
- Analysis of PNT systems to fulfill NSPD-39 requirements
- Competent PNT framework
- Fiscal Year 18 PNT Demonstration
- Normalization of PNT in risk management decisions
- Secure and Resilient Infrastructure

Homeland Security

For more information, visit:
www.dhs.gov/critical-infrastructure

James Platt
James.Platt@hq.dhs.gov
Mike Striffolino
Michael.Striffolino@hq.dhs.gov