

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

Unclassified

Outline

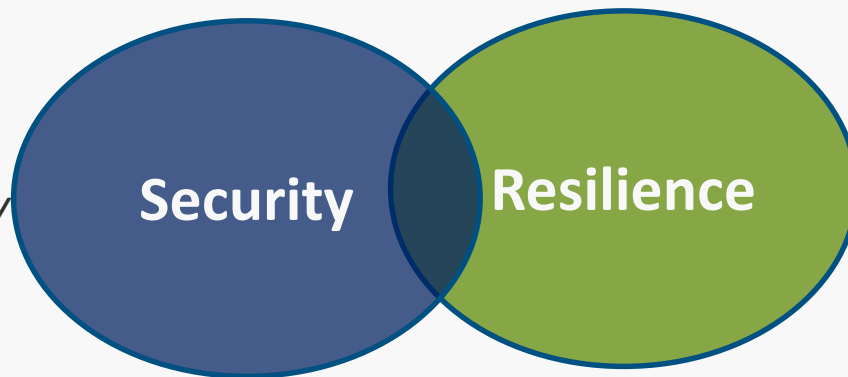
- DHS Role in Critical Infrastructure
- Timing in Critical Infrastructure
- Managing Risk
 - Holistic view of risk management
 - National Infrastructure Protection Plan (NIPP)
 - National Mitigation Framework
- Notional PNT architecture (FRP)
- Way ahead



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**

Unclassified

Presenter's Name June 17, 2003

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

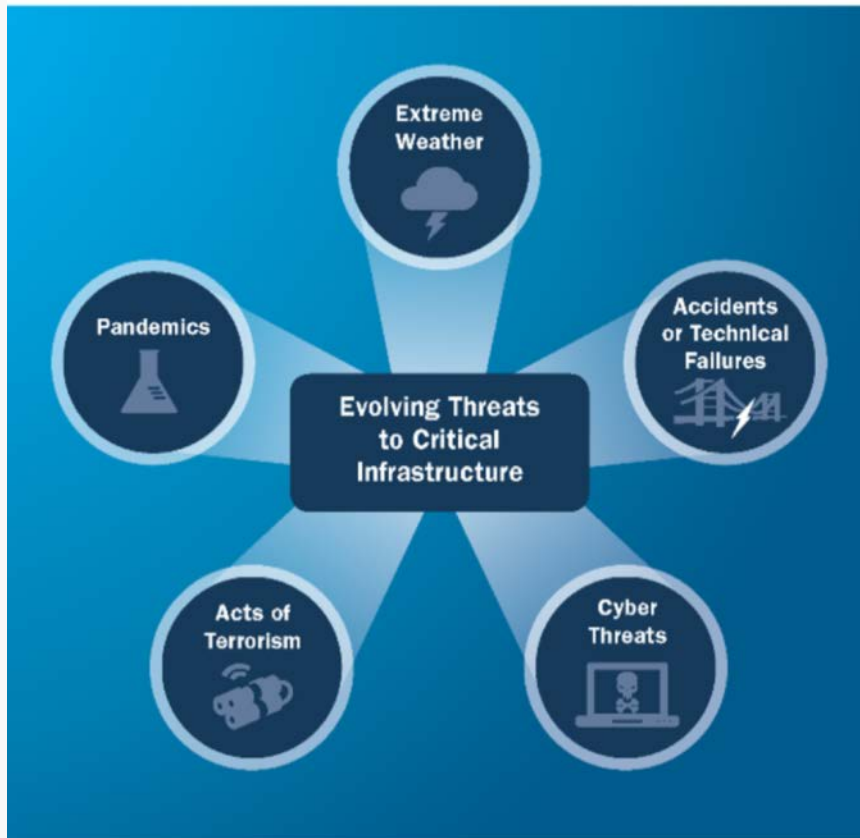


Do you need UTC? If yes, how do you get it? How do you operate without it?



**Homeland
Security**

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



**Homeland
Security**

Unclassified

Presenter's Name

June 17, 2003

6

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)

Owner-Operators

Customer Relations
Operations
Investment

State, Local, Regional

Public Safety
Law Enforcement
Utility Regulation



Federal Government

National Policy
Information Sharing
Coordination

NGOs

Trusted Relationships
Community Building
Research



**Homeland
Security**

UNCLASSIFIED

Presenter's Name

June 17, 2003

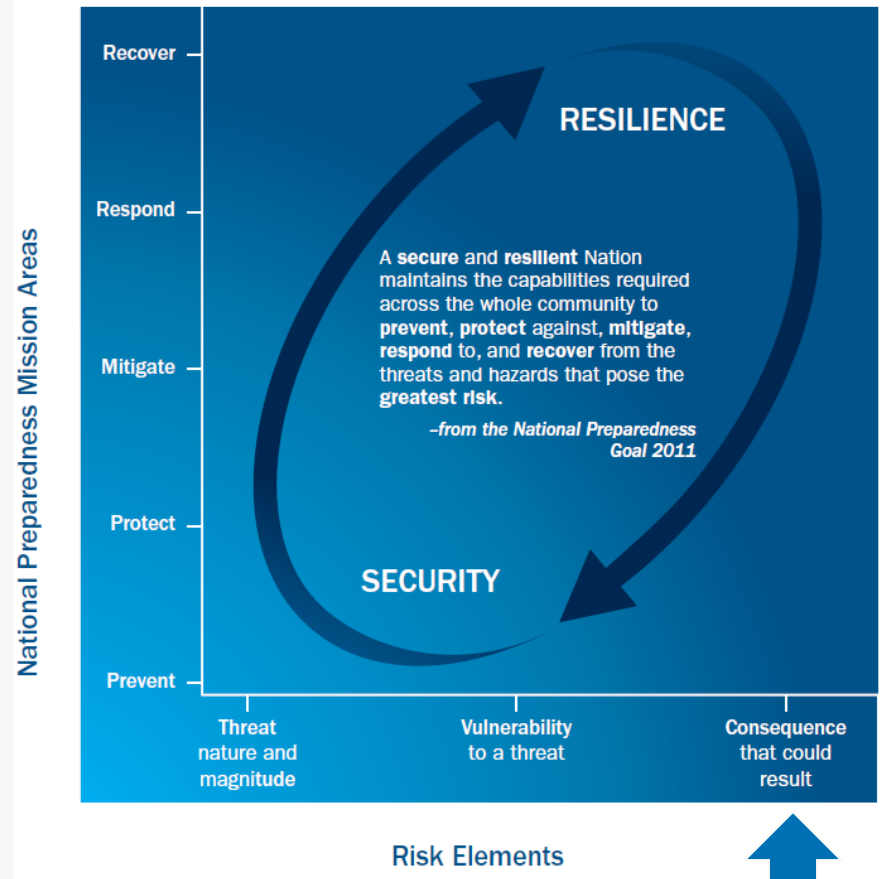
7

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



Homeland
Security

UNCLASSIFIED

Presenter's Name

June 17, 2003

8

The National Mitigation Framework

PNT Mitigation

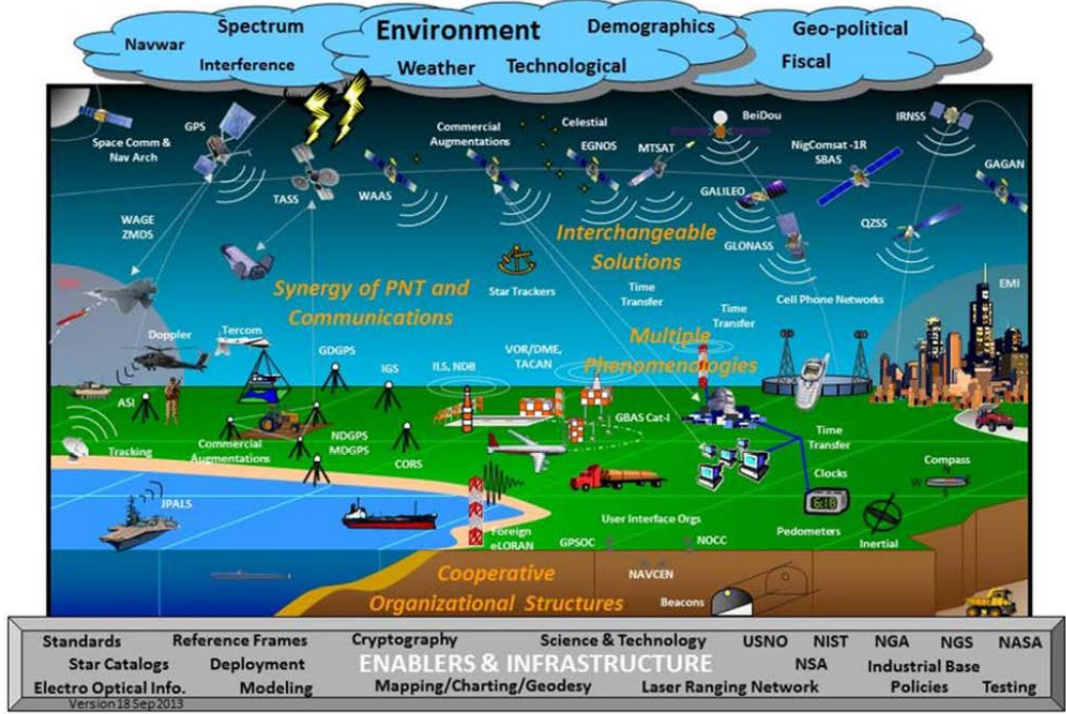
- Focus has been on Prevention and Protection
- Mitigation Efforts less energetic – more difficult
- How do we respond and recover?
- Do we understand where we fit in community efforts?
- When should we start thinking about mitigation (Hint: Design Phase)

Prevention	Protection	Mitigation	Response	Recovery
Planning				
Public Information and Warning				
Operational Coordination				
Intelligence and Information Sharing		Community Resilience Long-term Vulnerability Reduction Risk and Disaster Resilience Assessment Threats and Hazards Identification	Infrastructure Systems	
Interdiction and Disruption			Critical Transportation	Economic Recovery
Screening, Search, and Detection			Environmental Response/Health and Safety	Health and Social Services
Forensics and Attribution	Access Control and Identity Verification Cybersecurity Physical Protective Measures Risk Management for Protection Programs and Activities Supply Chain Integrity and Security		Fatality Management Services	Housing
			Fire Management and Suppression	Natural and Cultural Resources
			Logistics and Supply Chain Management	
			Mass Care Services	
			Mass Search and Rescue Operations	
			On-scene Security, Protection, and Law Enforcement	
			Operational Communications	
			Public Health, Healthcare, and Emergency Medical Services	
			Situational Assessment	



Federal Radionavigation Plan

National PNT Architecture (2025)



- 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 Strifolino

Michael.Strifolino@hq.dhs.gov