The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Department of Homeland Security Positioning Navigation, and
Timing Update

Civil GPS Service Interface Committee

September 13, 2016

Agenda

- GPS and Department of Homeland Security (DHS)

- Increasing Security and Resilience of Critical Infrastructure

- Positioning, Navigation, and Timing (PNT) in Critical Infrastructure

- Increasing Resilience of PNT

Homeland Security

Unclassified

Positioning, Navigation, and Timing

Essential to the Success of Homeland Security Missions

Courtesy of DHS

- Law Enforcement

- Border Protection

- Ports, Waterways, and Coastal Security

- Drug Interdiction

- Cybersecurity

- Emergency Management

Homeland Security

Unclassified

Securing and Enhancing PNT Capabilities

An Important Mission for Homeland Security

Courtesy of DHS

- Customs and Border Patrol

- National Protection and Programs Directorate (NPPD)

- DHS Science and Technology Directorate (S&T)

- United States Coast Guard

Homeland Security

National Protection and Programs Directorate

Managing Risks to the Nation's Cyber and Physical Infrastructure

- Managing risks to physical and cyber infrastructure and coordinating those efforts with partners across the Nation through the **Office of Cybersecurity and Communications** and the **Office of Infrastructure Protection (IP)**

- Protecting Federal facilities through the **Federal Protective Service** and establishing standards and best practices for Federal facility security through the **Interagency Security Committee**

- Developing all-hazards consequence analysis in the **Office of Cyber and Infrastructure Analysis**

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.
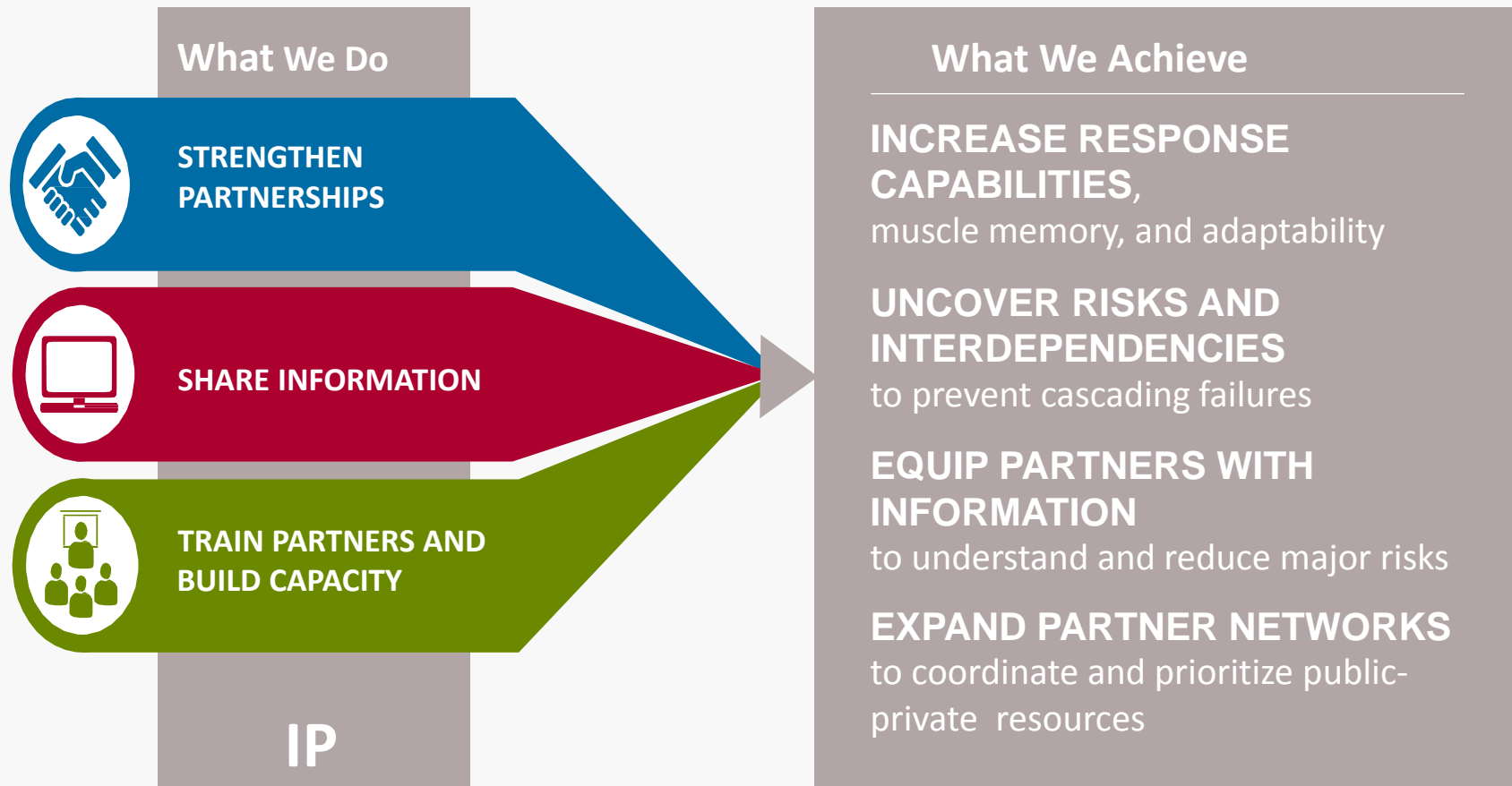
Courtesy of DHS

Comms. Sector

Critical Manufacturing

Government Facilities

Emergency Services

Nuclear Reactors, Materials & Waste

Energy Sector

Food & Agriculture

Defense Industrial Base

Transportation Systems

Dams Sector

Chemical Sector

Health & Public Health

Water & Wastewater

Information Technology

Commercial Facilities

Financial Services

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

How Does IP Achieve its Mission

What We Do

STRENGTHEN PARTNERSHIPS

SHARE INFORMATION

TRAIN PARTNERS AND BUILD CAPACITY

IP

What We Achieve

INCREASE RESPONSE CAPABILITIES, muscle memory, and adaptability

UNCOVER RISKS AND INTERDEPENDENCIES to prevent cascading failures

EQUIP PARTNERS WITH INFORMATION to understand and reduce major risks

EXPAND PARTNER NETWORKS to coordinate and prioritize public-private resources

The mission is to lead the national effort to protect critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.

Homeland Security

Our Economy Depends on Critical Infrastructure. Our Infrastructure Depends on GPS…Especially Timing.
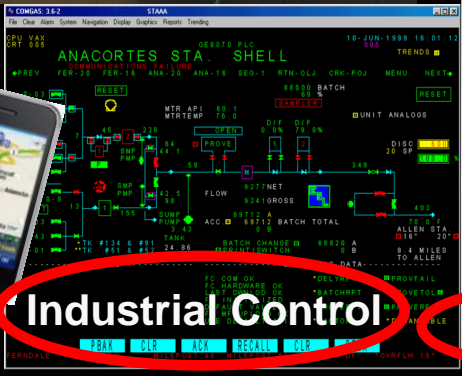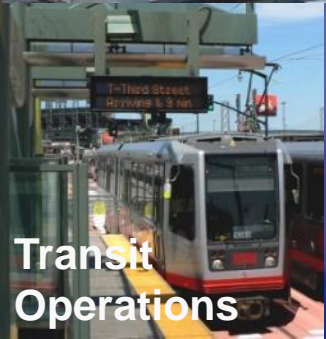
Strategies for Managing PNT Risk
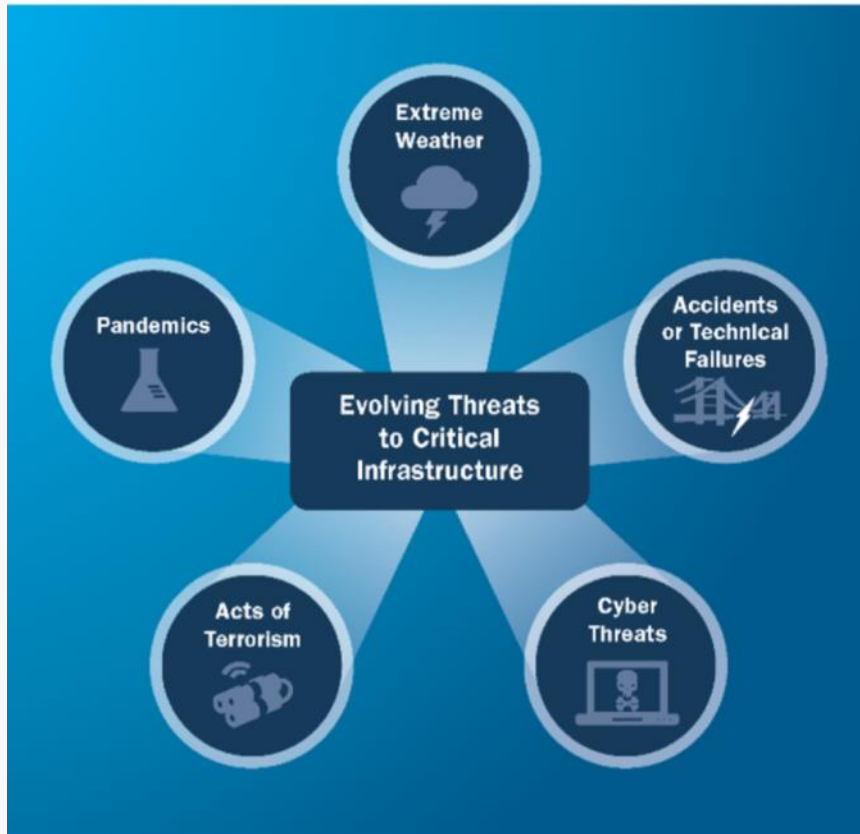
Courtesy of DHS

- 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

Homeland Security

2016: NPPD Accomplishments

National Communications Coordination Center (NCC)

- Within the National Cybersecurity and Communications Integration Center (NCCIC), the NCC represents DHS in interagency interference, detection, and mitigation efforts
  - Participant in exercises and other activities to ensure coordinated and efficient response to disruption events
  - Working to update and implement reporting and response processes
  - Key to 25 January 2016 GPS offset communication, coordination

- NCCIC maintains best practices documents focused on critical infrastructure use of PNT equipment
  - New best practices: leap second and technical note on timing

Access Best Practices Documents at https://ics-cert.us-cert.gov

Homeland Security

Unclassified

2016: NPPD Accomplishments

IP PNT Program Management Office

- Successful first year of the IP PNT PMO

- Leading DHS Participation in interagency Complementary Positioning, Navigation, and Timing Tiger Team
  - Co-sponsoring a study gathering PNT requirements for critical infrastructure sectors

- Expanding reach to owners and operators of critical infrastructure
  - Provided in-depth training for 100+ field staff and regional directors on critical infrastructure use of PNT and threats and vulnerabilities facing GPS operations
  - Continuing direct engagement with critical infrastructure owners and operators

Homeland Security

2016: DHS S&T Accomplishments

PNT Broad Agency Agreement (BAA)

- Title: Assured Timing for Critical Infrastructure (BAA Call HSHQDC-15-R-B0008)

- Proposals Solicited for Three Technical Topic Areas:
    - Development of Assured Timing Technologies
    - System-Level Testing and Analysis to Understand Impacts
    - Development of Timing Manipulation Detection Capabilities

Conducting Research, Development, and Commercialization of Products to Improve the Nation's Security and Resilience

2016: DHS S&T Accomplishments

Cooperative Research and Development Agreement (CRADA)

- Purpose: Test potential of eLORAN as a complementary PNT solution for critical infrastructure applications

- Participants: DHS S&T, Coast Guard, UrsaNav, and Harris Corp.

- Executed a demonstration of eLORAN at the New York Stock Exchange (NYSE) on April 19, 2016
  - Signal received inside NYSE holding within 30 nanoseconds of UTC where GPS was not receivable

- CRADA extended until May 2017 to study performance impacts to signal traveling over varied terrain

Homeland Security

Looking Forward to 2017

- Education and Engagement
  - Publication of Best Practices Documents (Fall 2016)
  - Development of Materials for First Responder Community
  - Direct Engagement with PNT Industry Community

- Research and Development Efforts
  - CRADA
  - Expanding Breadth of R&D through BAA
  - Vulnerability Testing

- Requirements Study of Critical Infrastructure PNT Use

Homeland Security

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

Greg Carden
Gregory.Carden@hq.dhs.gov
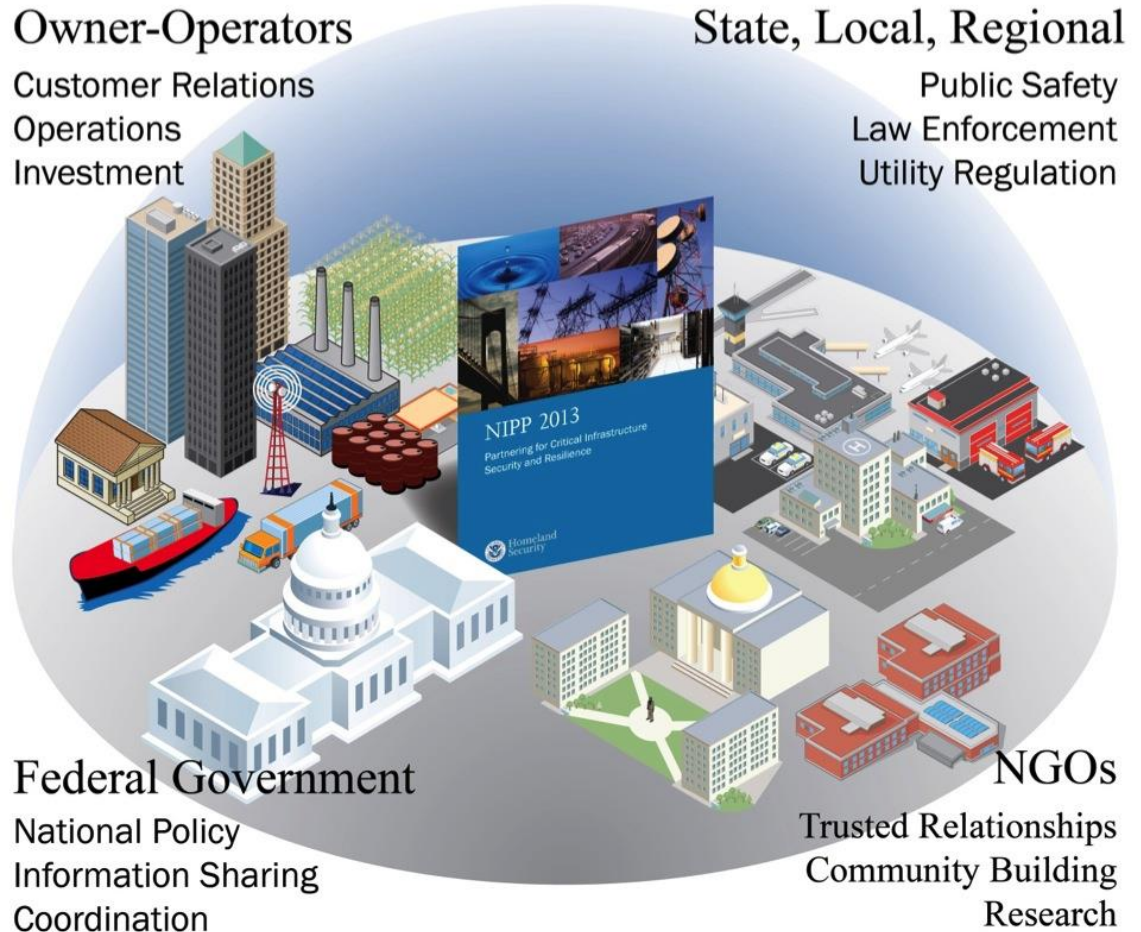**John Dragseth**
John.Dragseth@hq.dhs.gov

Backup

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

Comparative Advantage

- Engaging in collaborative processes
- Applying individual expertise
- Bringing resources to bear
- Building the collective effort
- Enhancing overall effectiveness

Courtesy of DHS

Owner-Operators
Customer Relations
Operations
Investment

State, Local, Regional
Public Safety
Law Enforcement
Utility Regulation

NIPP 2013
Partnering for Critical Infrastructure
Security and Resilience

Federal Government
National Policy
Information Sharing
Coordination

NGOs
Trusted Relationships
Community Building
Research

Critical Infrastructure Depends on GPS

Power Grid Systems

Transportation Centers

Banking Operations

Communications Systems

Homeland Security

What We Know About GPS in Critical Infrastructure

- GPS is used in every critical infrastructure, and its use continues to expand

- Timing is the most critical aspect of PNT for critical infrastructure operations, and GPS is over-relied upon for that information

- We anticipate that impacts due to most scenarios will be limited
  - Impacts will expand if GPS is not available for longer durations
  - Consistent GPS service means we have no way to confirm the impacts of a GPS outage
  - Many sectors have less risk to a GPS interruption than commonly portrayed in the GPS community

Homeland Security

Unclassified

DHS is Conducting Jamming and Spoofing Testing

- Testing:

    - Focusing on GPS equipment used for precision timing in critical infrastructure operations

    - Examining test results to better understand potential equipment impacts

Homeland Security

Unclassified