The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

GPS and Critical Infrastructure

Civil GPS Service Interface Committee

September 15, 2015

Homeland Security

Unclassified

Agenda

- GPS and Department of Homeland Security (DHS)
- Critical Infrastructure Security and Resilience
- Positioning, Navigation, and Timing (PNT) in Critical Infrastructure
- Increasing Resilience of PNT

Positioning, Navigation, and Timing

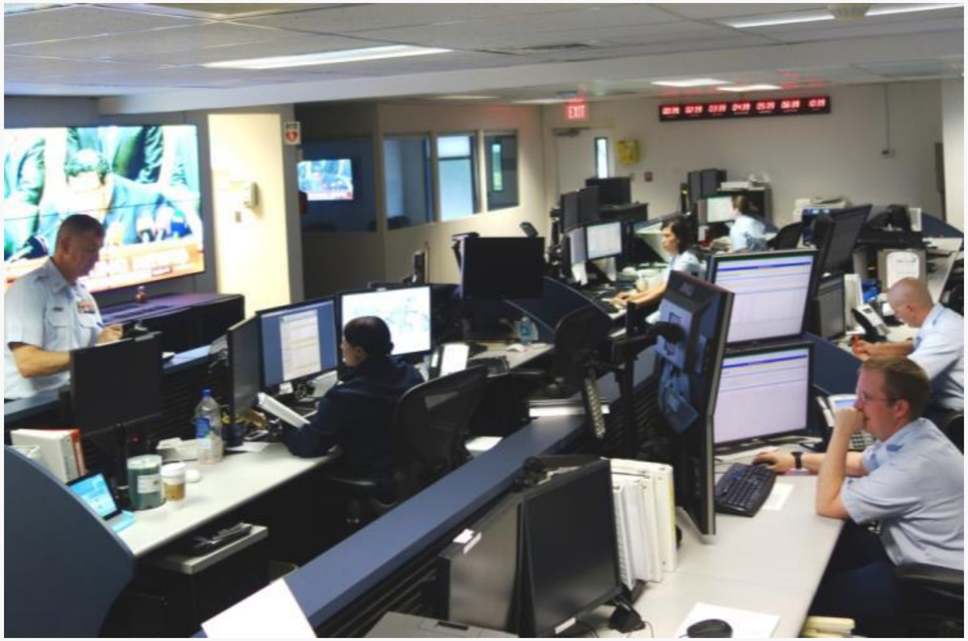
A Key DHS Mission Area and Essential to our Success

Courtesy of DHS

- Infrastructure Protection
- Law Enforcement
- Border Protection
- Ports, Waterways, and Coastal Security
- Drug Interdiction
- Cybersecurity
- Emergency Management
- Science and Technology

United States Coast Guard

The Interface to Civil GPS Users Worldwide



Courtesy of DHS

- Maintains the Nation’s maritime aids to navigation
- The Coast Guard Navigation Center (NAVCEN)
  - Entry-point for civil & commercial GPS users reporting GPS issues
  - Whole-of-government coordination with DoD’s GPSOC and Federal Aviation Administration’s National Operation Control Center for interference events

NAVCEN GPS Problem Reporting:
http://www.navcen.uscg.gov/?pageName=gpsUserInput

Customs and Border Patrol

Prevents GPS Jammer Importation and Use in Supply Chain

Courtesy of DHS

- Multi-layered cargo enforcement
  - Inspections
  - Advisories
  - Industry partnerships
- Relationship with the U.S. Federal Communications Commission (FCC) enables enforcement actions

Science and Technology Directorate

Confirms GPS Vulnerabilities and Develops Mitigations

- Science and Technology Directorate (S&T) coordinates numerous projects related to positioning, navigation, and timing
  - Jamming and spoofing testing of GPS receivers
  - Alternate sources of distributing precision time
  - Technologies to identify GPS disruption
  - Deepening understanding of PNT operational requirements
- S&T develops research priorities in coordination with DHS components with the goal of commercializing developed products

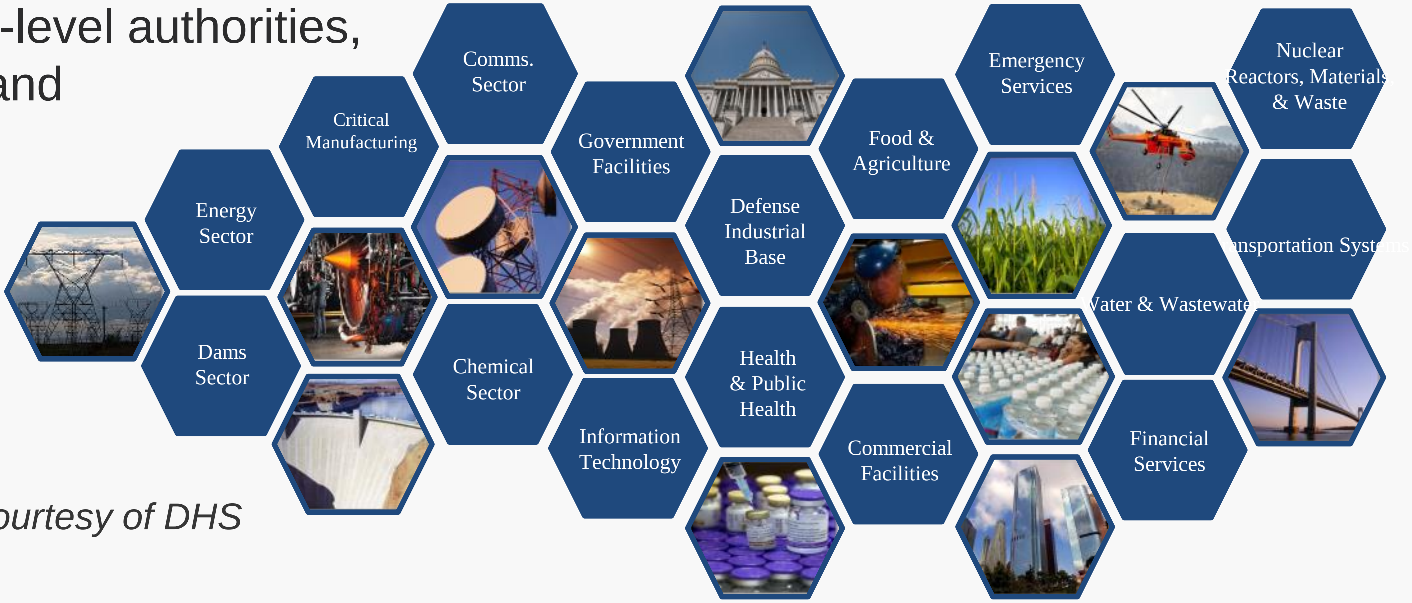
National Protection and Programs Directorate

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**
- 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**

DHS 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.



Energy Sector

Dams Sector

Critical Manufacturing

Comms. Sector

Chemical Sector

Government Facilities

Information Technology

Defense Industrial Base

Health & Public Health

Food & Agriculture

Commercial Facilities

Emergency Services

Water & Wastewater

Financial Services

Nuclear Reactors, Materials & Waste

Transportation Systems

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."

Our Economy Depends on Critical Infrastructure and Our Infrastructure Depends on GPS

Surveying & Mapping

Power Grids

Precision Agriculture

Space Applications

Air Traffic Control

Healthcare

Emergency Services

Transit Operations

Telecom

Trucking

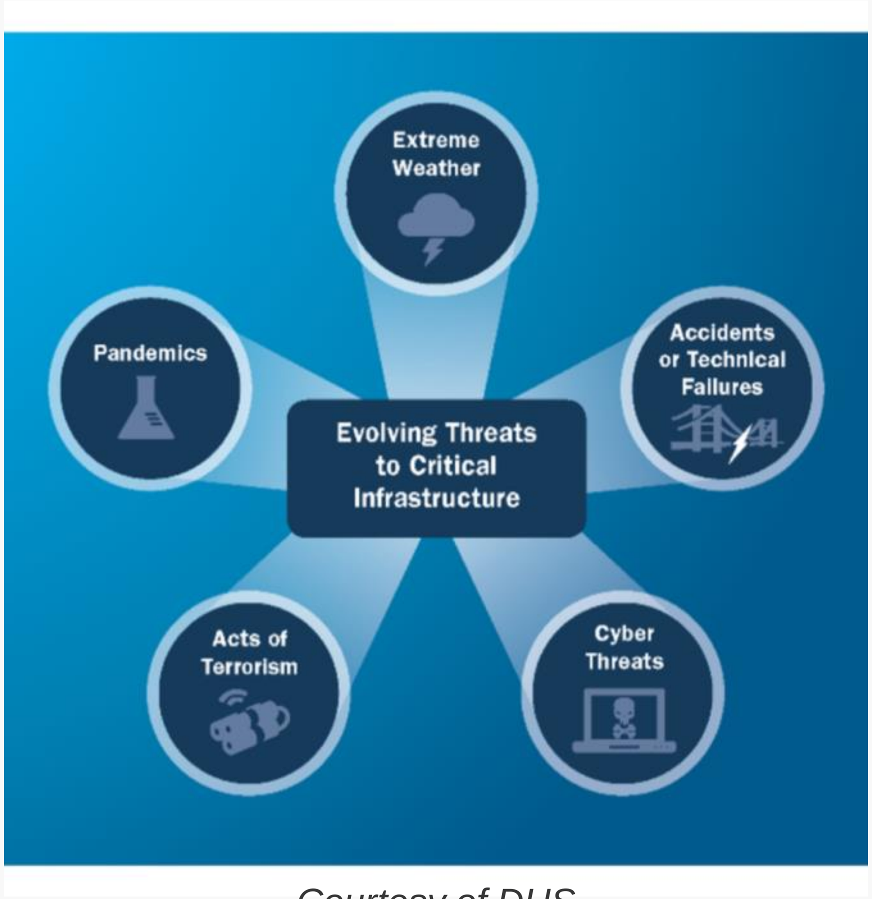
Financial Markets

Personal Navigation

Shipping & Maritime Applications

Oil Exploration

Strategies for Managing PNT Risk


Extreme Weather
Pandemics
Accidents or Technical Failures
Evolving Threats to Critical Infrastructure
Acts of Terrorism
Cyber Threats

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)
- Engaging Key Stakeholders
- Exploring new technologies

DHS is Conducting Jamming and Spoofing Testing and Providing Best Practices to the Critical Infrastructure Community

- Testing:
  - Focusing on GPS equipment used for precision timing in critical infrastructure operations
  - Examining test results to better understand potential equipment impacts
- Best Practices Documents: Two published, more to come
  - *Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations*
  - *Best Practices for Leap Second Event Occurring 30 June 2015*

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

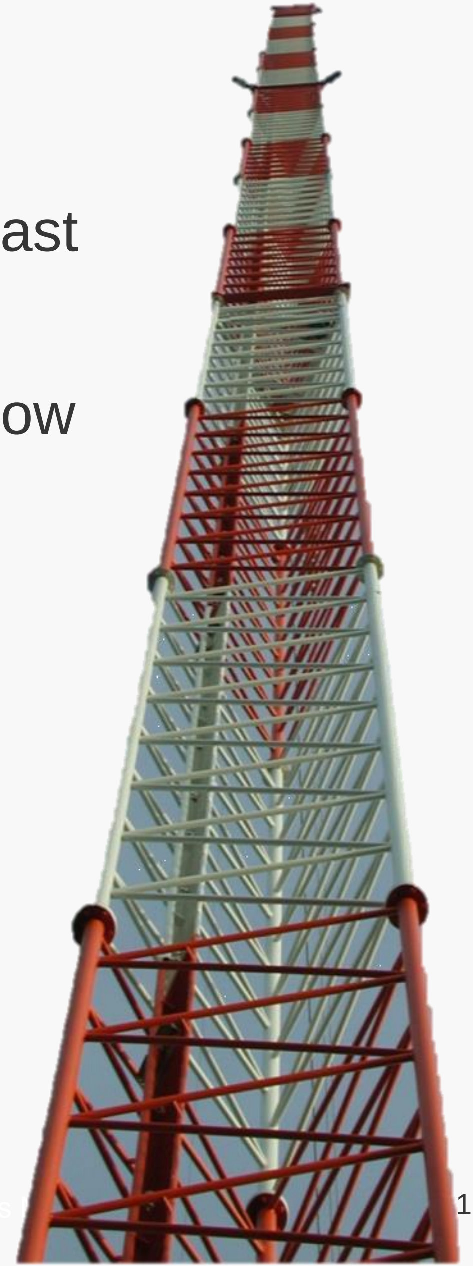
An Interagency Team is Examining Complementary PNT Capabilities to Supplement GPS

- Space-Based PNT Executive Committee (at the Deputy Secretary level) looked at the need for a complement to GPS
  - Assessment driven by many factors: from natural to manmade events considering policies and technologies
- Decisions and timelines support FY17 investment decisions
- Public comment focused on the need for a complement to GPS was solicited via a Federal Register Notice which closed on May 22, 2015

Review public comments at www.regulations.gov by searching DOT-OST-2015-0053

eLORAN CRADA

- The Cooperative Research and Development Agreement (CRADA) was co-signed by the Coast Guard, S&T, Harris, and UrsaNav
- Key objective: demonstrate the potential for a low frequency terrestrial application of PNT using former Loran-C stations
- Operating in the 90-110 kHz band
- CRADA duration is three years



Courtesy of DHS

Looking Forward

- Critical Infrastructure PNT Program Management Office
- Expanded Research and Development Efforts

Homeland Security

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

John Dragseth

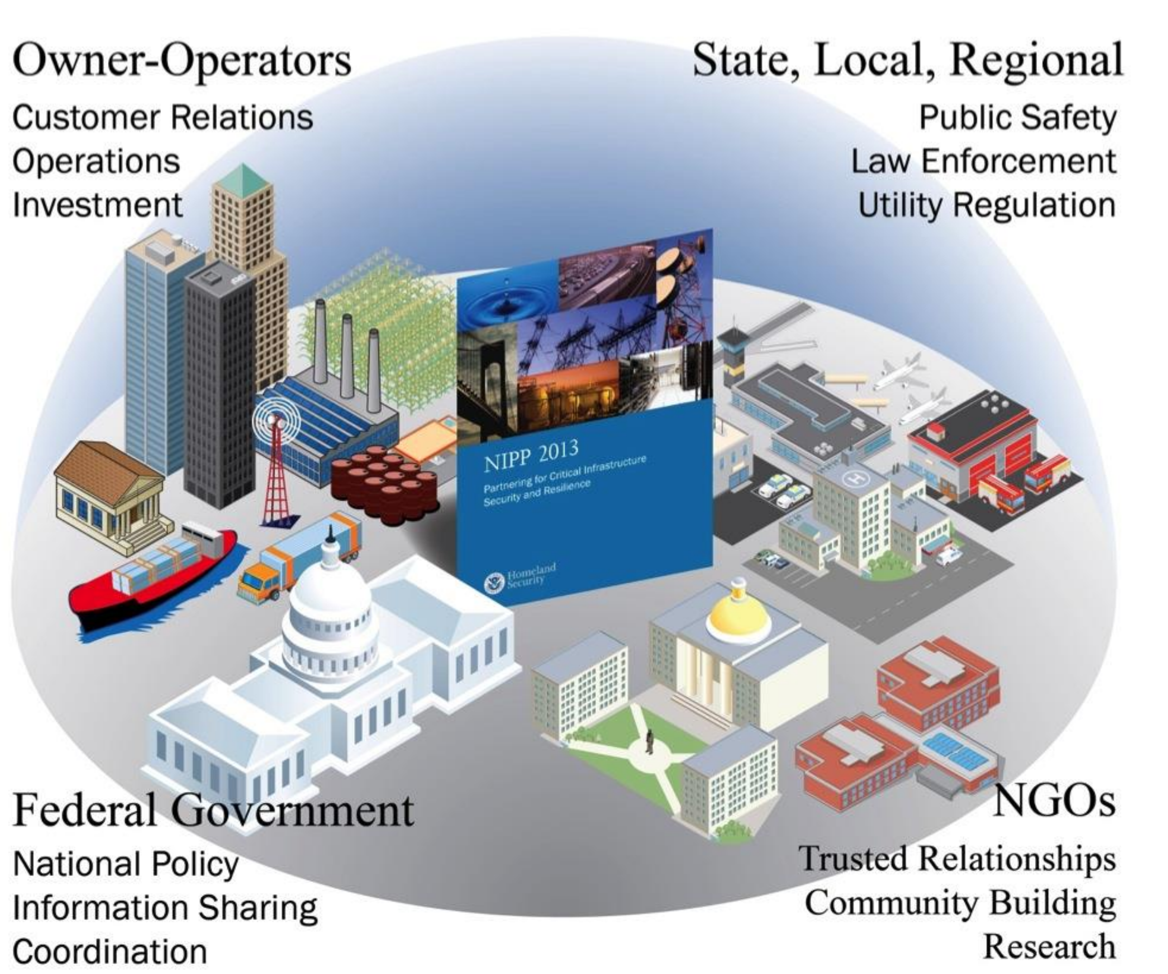
John.Dragseth@hq.dhs.gov

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



Owner-Operators

Customer Relations
Operations
Investment

State, Local, Regional

Public Safety
Law Enforcement
Utility Regulation

Federal Government

National Policy
Information Sharing
Coordination

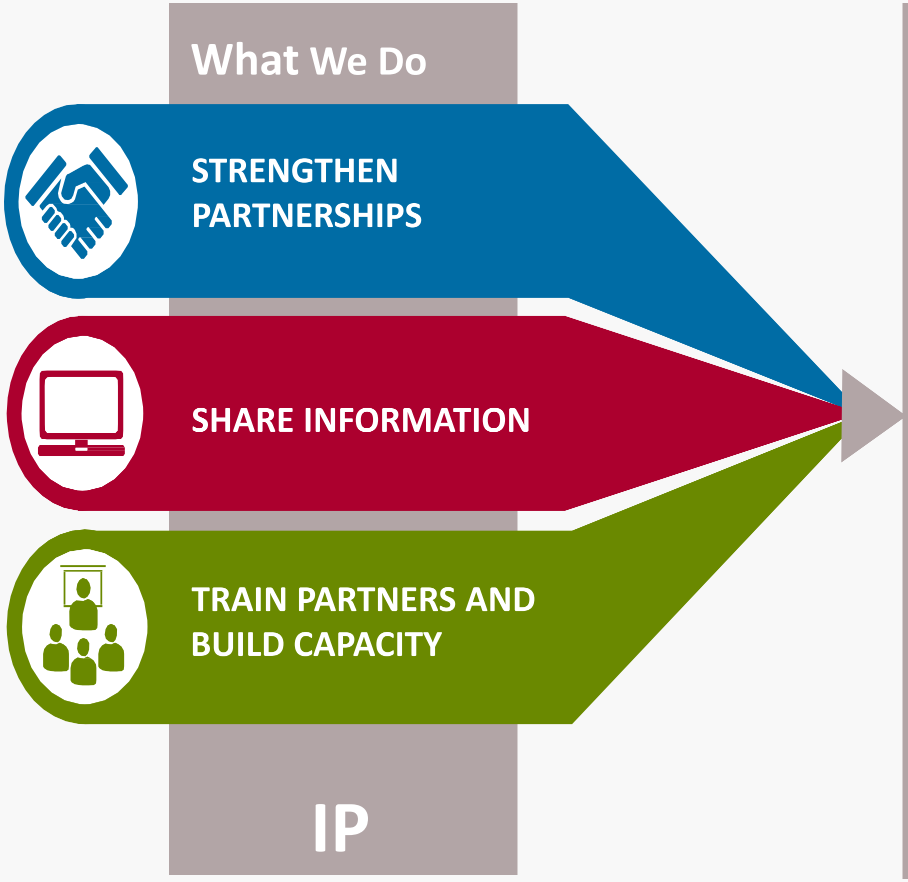
NGOs

Trusted Relationships
Community Building
Research

NIPP 2013
Partnering for Critical Infrastructure Security and Resilience
Homeland Security

Courtesy of DHS

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.

UNCLASSIFIED

Critical Infrastructure Depends on GPS

Power Grid Systems

Banking Operations

Transportation Centers

Communications Systems

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