U.S. Department of Homeland Security
in partnership with the
National Coordination Office for Space-Based Positioning, Navigation and Timing

Critical Infrastructure Security and Resilience

International Committee on Global Navigation Satellite Systems

November, 2014

Homeland Security

SPACE-BASED POSITIONING NAVIGATION & TIMING

NATIONAL COORDINATION OFFICE

Agenda

- GPS and the U.S. Critical Infrastructure
- U.S. Approach to Critical Infrastructure Security and Resilience
- International Critical Infrastructure

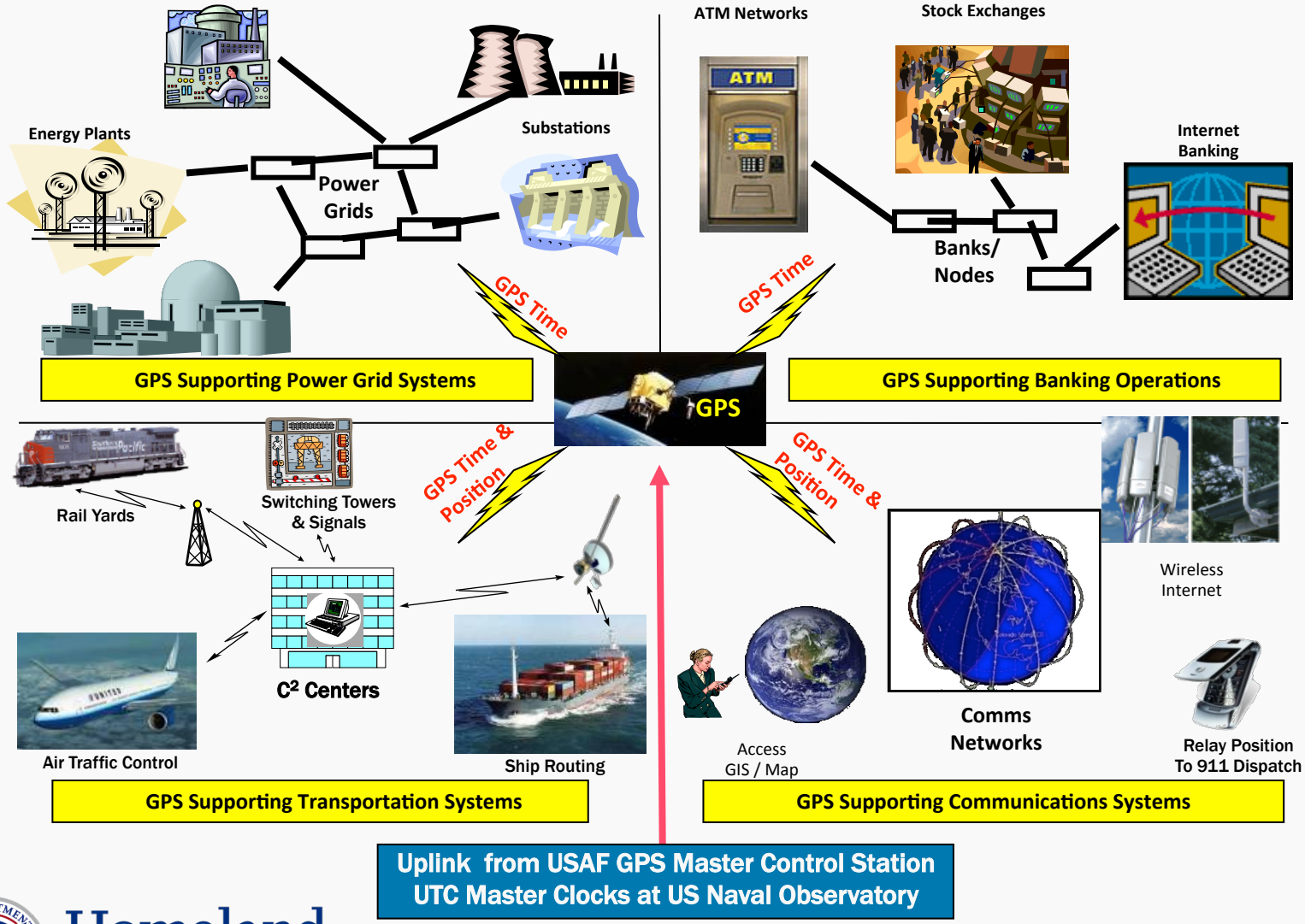
Homeland Security

U.S. GPS Today

- Primary distribution for time and frequency in the U.S. and the world
- Enables increased mobility and innovation in critical infrastructure
- Evolution of GPS dependencies:
  - Incorporated into broadly-used mobile devices
  - Integrates with other technologies, including Geographic Information Systems, remote sensing, and precision location technologies
  - Advances efficiencies in operations and supply chains

Homeland Security

GPS and U.S. Critical Infrastructure



Homeland Security

Department of Homeland Security –
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

United States Critical Infrastructure

Critical Infrastructure includes distributed networks, 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.

16 Critical Infrastructure Sectors in the U.S.

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food & Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water & Wastewater Systems

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

National Policies

President Barack Obama signed two policies related to critical infrastructure security and resilience in February 2013:

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience

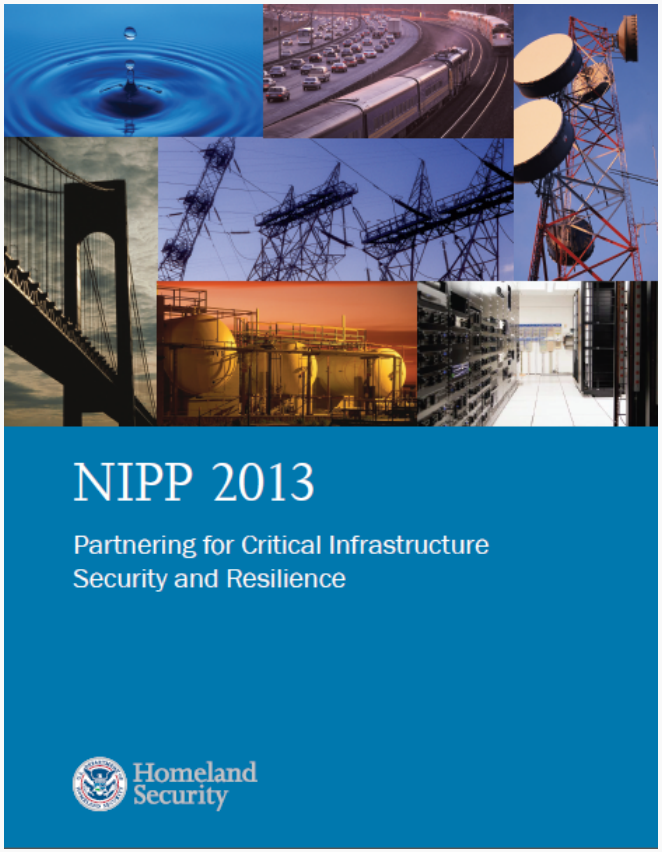
Executive Order 13636: Improving Critical Infrastructure Cybersecurity

"The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure that are vital to public confidence and the Nation's safety, prosperity, and well-being."

– Presidential Policy Directive (PPD) 21

Homeland Security

National Infrastructure Protection Plan - 2013

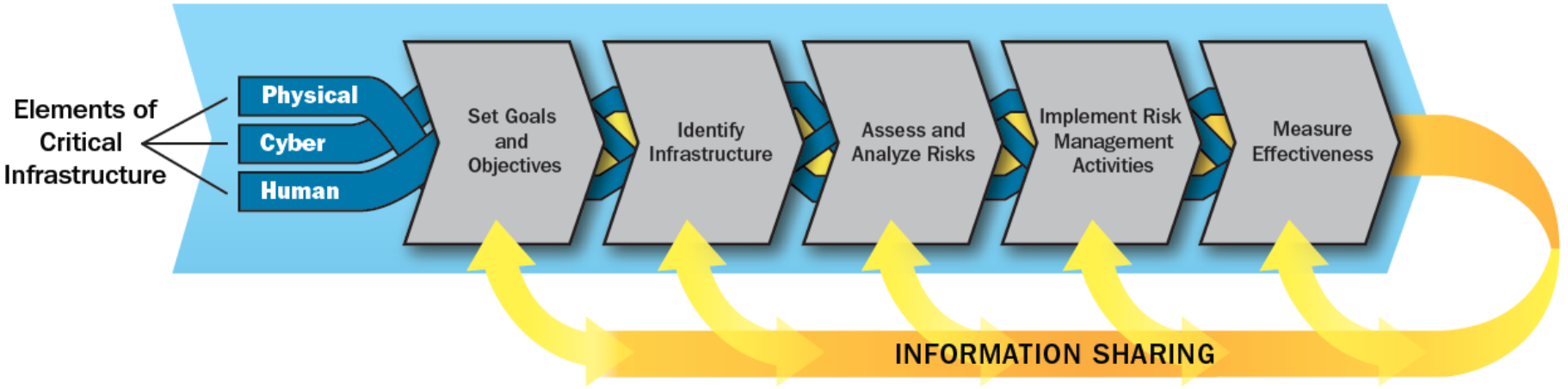


Courtesy of DHS

- Provides strategic guidance for the national effort to enhance security and resilience through critical infrastructure community collaboration:
  - Applies a risk management focus
  - Promotes collective action through partnerships
  - Outlines authorities, roles and responsibilities
- Guides DHS programs and activities and those of:
  - Federal departments and agencies
  - State, local, tribal, and territorial governments
  - Regional organizations and partnerships
  - Critical infrastructure owners and operators
  - Other critical infrastructure stakeholders (e.g., academia, non-profit organizations)
- Vision: A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.

Homeland Security

Risk Management Framework



Critical Infrastructure Risk Management Framework

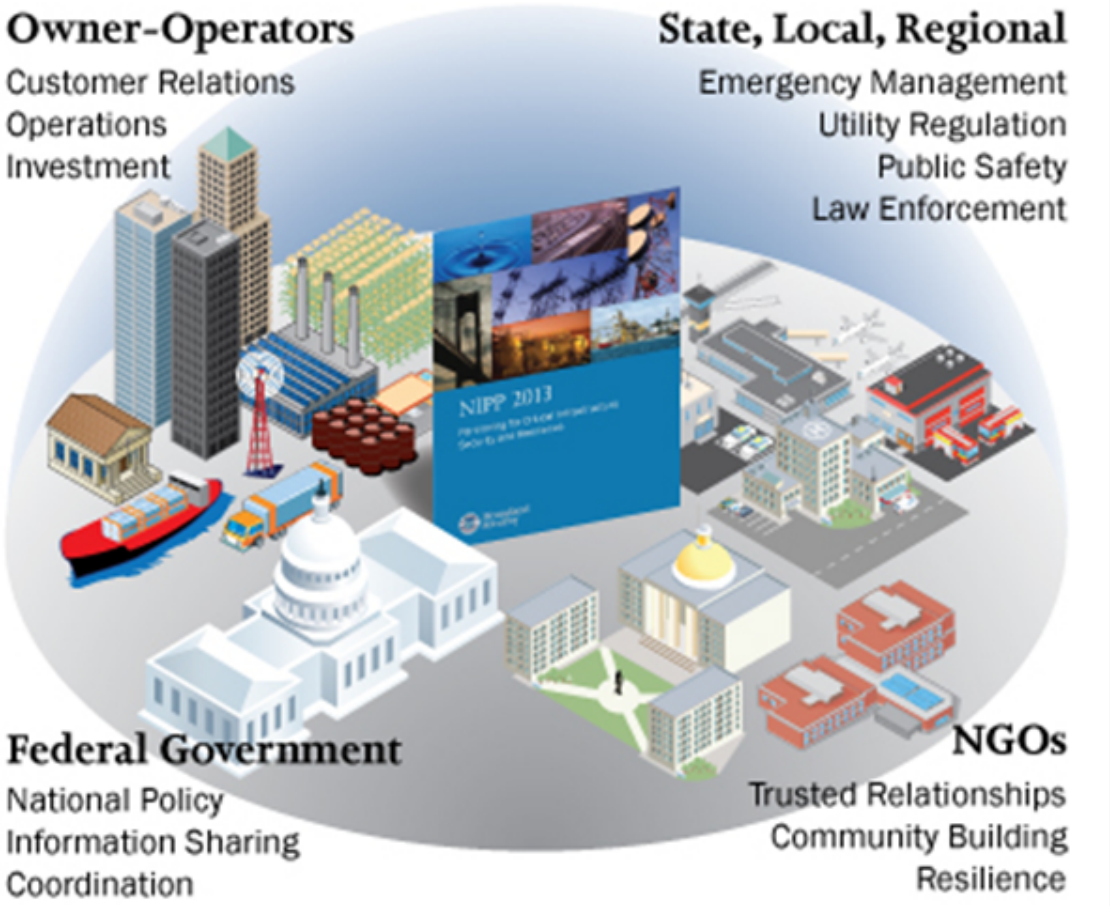
- Partners benefit from access to knowledge and capabilities that would otherwise be unavailable to them
- Risk tolerances and priorities will vary
- Costs and benefits considered during decision making
- Information sharing integrated as core component of risk management

Homeland Security

Many Stakeholders, Many Strengths

Comparative Advantage

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



Homeland Security

International Partners in

Critical Infrastructure Security and Resilience

- Resilience – stakeholders, interdependencies, and risk environment change over time and conditions. Continually seek to build upon:
  - relationships with foreign infrastructure
  - streamlined supply chains
- PPD-21 provides for State Department, DHS and others:
  - Engage with foreign governments and organizations
  - Exchange best practices and lessons learned
  - Promote security and resilience of critical infrastructure
- Bilateral work with Public Safety Canada
- Multilateral work through:
  - Partnership with Canada, UK, Australia, New Zealand
  - Asia Pacific Economic Cooperation (APEC) economies
  - European Union – US – Canada Experts meeting
  - North Atlantic Treaty Organization (NATO) - Industrial Resources Communication Services Group (IRCSG)

Homeland Security

Pursuing Resilient P, N, T…

- If a disruption were to occur to GPS civil services, the U.S. goal is to restore the essential functions of the economy, society, and government, as quickly as possible.
- In other words, pursue self-healing P, N, T architectures and infrastructures (system-of-systems) that bend, rather than break, in the face of a disruption.

Resilience: The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (Source: NIPP, 2013 & PPD-21, 2013)

Homeland Security

Homeland Security

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

John Dragseth

Office of Infrastructure Protection
Strategy and Policy

John.Dragseth@hq.dhs.gov