SPACE-BASED POSITIONING
NAVIGATION & TIMING

NATIONAL COORDINATION OFFICE

U.S. Space-Based Positioning, Navigation and Timing (PNT) Policy Update

Open PNT Industry Alliance
9 February 2022

Harold W. Martin III
Director
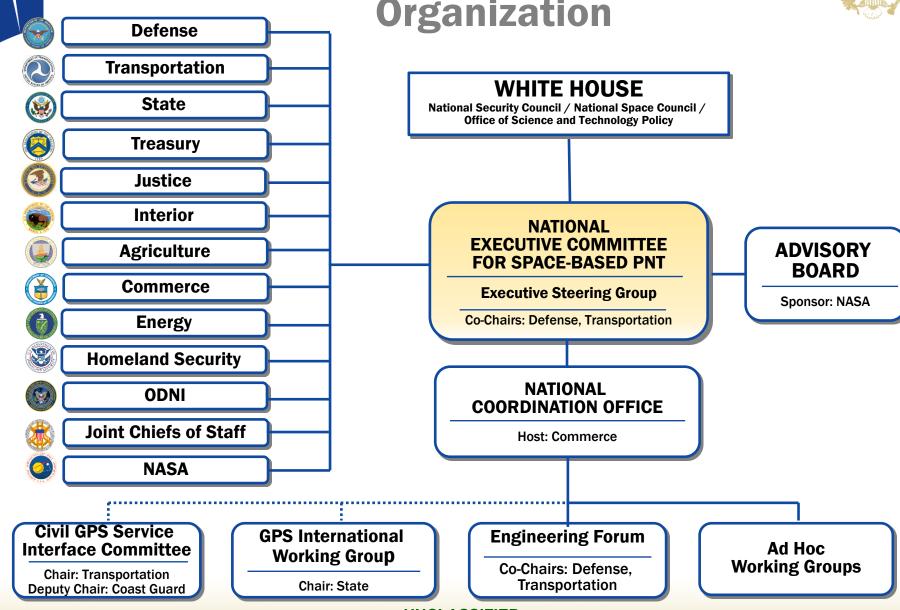National Coordination Office

Overview

- **National Space-Based PNT Organization**

- **U.S. Policy**
  - **SPD-7**
  - **National Space Policy**
  - **EO-13905**
  - **SPD-5**

- **The Airwaves are Not Safe**

National Space-Based PNT Organization

Defense

Transportation

State

Treasury

Justice

Interior

Agriculture

Commerce

Energy

Homeland Security

ODNI

Joint Chiefs of Staff

NASA

WHITE HOUSE
National Security Council / National Space Council /
Office of Science and Technology Policy

NATIONAL EXECUTIVE COMMITTEE FOR SPACE-BASED PNT

Executive Steering Group

Co-Chairs: Defense, Transportation

ADVISORY BOARD

Sponsor: NASA

NATIONAL COORDINATION OFFICE

Host: Commerce

Civil GPS Service Interface Committee

Chair: Transportation
Deputy Chair: Coast Guard

GPS International Working Group

Chair: State

Engineering Forum

Co-Chairs: Defense, Transportation

Ad Hoc Working Groups

Space Policy Directive 7 (SPD-7)
of 15 January 2021

> **Updates and replaces U.S. Space-Based PNT Policy of 2004**

- Increased focus on protecting GPS and denying hostile use

- Incorporated principles of Responsible Use of GPS

- New direction on adding cybersecurity protections for GPS and federal user equipment

- Expanded EXCOM Membership
  - Added Departments of Treasury, Justice, and Energy

- New direction to protect the GPS spectrum environment

U.S. Policy

> The goal of [SPD-7] is to maintain United States leadership in the service provision, and responsible use of, global navigation satellite systems (GNSS), including GPS and foreign systems.

- Continuous, worldwide, free of direct user fees

- Encourage compatibility and interoperability with like-minded nations, promote transparency in civil service provisioning and enable market access for United States industry

- Operate and maintain constellation to satisfy civil and national security needs and equip and train for the responsible use of GPS

  - Foreign PNT services may augment and strengthen the resiliency of GPS; however, the US Government does not assure the reliability or authenticity of foreign PNT services

- Invest in domestic capabilities and support international activities to detect, mitigate and increase resiliency to harmful interference

- Improve the cybersecurity of GPS, its augmentations, and United States Government-owned GPS-enabled devices, and foster private sector adoption of cyber-secure GPS enabled systems

SPD-7 Changes to Agency Responsibilities

- *State*
  - New mention of cooperation with DoD in relations with Allies

- *Defense*
  - Direction to work with DOT to maintain "safety-of-life backwards compatibility commitments"
  - Direction to provide cost estimates to the GPS program based on DOT's strategy and future requirements to implement GPS data and signal authentication.
  - New mention of existing role as lead for International Spectrum Coordination

- *Commerce*
  - Direction to Invest in R&D for enhancing commercial services
  - Direction to develop cybersecurity resilience guidelines

SPD-7 Changes to Agency Responsibilities

- *Transportation*
  - Direction to ensure the earliest availability of modernized civil signals
  - New direction to implement Federal and facilitate State, local and commercial capabilities to monitor, identify, locate, and attribute space-based PNT service disruption and manipulations within the U.S.
  - Direction to develop international signal monitoring standards
  - New caution on the use of foreign GNSS
  - New direction to pursue data and signal authentication

- *Homeland Security*
  - Added reference to EO13905 on Responsible Use of PNT
  - Direction to develop procedures for notification of disrupted and/or unreliable PNT
  - Direction to assist DOT in implementing data and signal authentication

National Space Policy
9 December 2020

The U.S. must maintain its leadership in the service, provision, and responsible use of global navigation satellite systems (GNSS)

- Provide continuous worldwide access for peaceful civil uses free of direct user fees;

- Engage with international GNSS providers to ensure compatibility, encourage interoperability with like-minded nations, promote transparency in civil service provision, and enable market access for United States industry;

- Operate and maintain the GPS constellation to satisfy civil and national security needs,

- Improve the cybersecurity of GPS, its augmentations, and federally-owned GPS enabled devices,

- Allow for the continued use of allied and other trusted international PNT services in conjunction with GPS

National Space Policy
(cont.)

- Invest in domestic capabilities and support international activities to detect, analyze, mitigate, and increase resilience to harmful interference to GNSS;

- Identify and promote, as appropriate, multiple and diverse complementary PNT systems or approaches for critical infrastructure and mission-essential functions; and

- Promote the responsible use of United States space-based PNT services and capabilities in civil and commercial sectors at the Federal, State, and local levels, including the utilization of multiple and diverse complementary PNT systems or approaches for national critical functions.

Executive Order 13905
of 12 February 2020

Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services

"Responsible use of PNT services" –
Means the deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government.

Space Policy Directive 5 (SPD-5)
of 4 September 2020

Establishing space cybersecurity policy, standards, and risk management practices

"…the United States considers unfettered freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation…Therefore, it is essential to protect space systems from cyber incidents in order to prevent disruptions to their ability to provide reliable and efficient contributions to the operations of the Nation's critical infrastructure."

The Airwaves Are Not Safe

- Computers and the Internet: Once Upon a Time…
  - A GPS receiver is more computer than radio…
- GPS relies on spectrum – no longer a safe haven
- 900 Million U.S. GPS enabled devices require Cybersecurity
- U.S. Policy directs PNT resiliency (SPD-5, SPD-7, PPD-21, EO 13800, EO 13905, National Cyber Strategy)
- NIST PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of PNT Services (NISTIR 8323)

"Known but unmitigated vulnerabilities are among the highest cybersecurity risks…"

(EO 13800: Strengthening the Cybersecurity of Federal Networks and

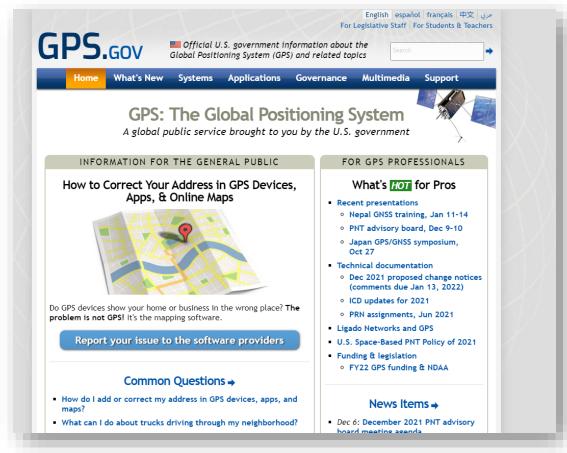*Critical Infrastructure)*

What Can You Do Now?

- CIOs: Include GPS enabled devices in Cybersecurity plans

- Be a demanding customer - toughen GPS devices:
  - Incorporate valid range checking and other elements of GPS Interface Specification (IS-GPS-200M *)
  - Incorporate DHS Best Practices (*Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure, Jan 2017 *)*

  * Documents available on www.gps.gov

Protect GPS and Critical Infrastructure that Relies on GPS

Thank You

Stay in touch:
www.gps.gov

Contact Information:
National Coordination Office

for Space-Based PNT

1401 Constitution Ave, NW

Room 62028

Washington, DC 20230

Email: pnt.office@gps.gov

Phone: (202) 482-5809

GPS: Accessible, Accurate, Interoperable