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

58th Meeting of the Civil GPS Service Interface Committee
Miami, Florida

25 September 2018

Harold W. Martin III
Director
National Coordination Office
The U.S. must maintain its leadership in the service, provision, and use of Global Navigation Satellite Systems (GNSS)

- Continuous, worldwide, free of direct user fees
- Encourage compatibility and interoperability with foreign GNSS services and promote transparency in civil service provisioning
- Operate and maintain constellation to satisfy civil and national security needs
  - Foreign PNT services may be used to augment and strengthen the resiliency of GPS
- Invest in domestic capabilities and support international activities to detect, mitigate and increase resiliency to harmful interference
National Space-Based PNT Organization

WHITE HOUSE

NATIONAL EXECUTIVE COMMITTEE FOR SPACE-BASED PNT

Executive Steering Group
Co-Chairs: Defense, Transportation

NATIONAL COORDINATION OFFICE
Host: Commerce

ADVISORY BOARD
Sponsor: NASA

Defense
Transportation
State
Interior
Agriculture
Commerce
Homeland Security
Joint Chiefs of Staff
NASA

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

3
EXCOM Strategic Focus Areas

- GPS Sustainment and Modernization
- International Cooperation
- Spectrum Management
- Critical Infrastructure
- PNT Resilience
- Outreach
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
- GPS receivers lack cyber resilience
- Policy directs PNT resiliency (NSPD-39, PPD-4, PPD-21)
- Jan 6, 2017 - DHS released Best Practices document now available on GPS.gov:
  "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure"

Protect GPS and Critical Infrastructure that Relies on GPS
GPS Cyber Resilience: Growing Issue

• GPS Receivers Lack Cyber Resilience
• Est. 600 Million GPS receivers in the U.S. today
  • National Security ~ 1%
  • Critical Infrastructure and Federal Systems ~ 1%
  • Private and Commercial ~ 98%
• Cross cuts communities

National Security  Critical Infrastructure & Fed Sys  Private & Commercial
International Users  Foreign GNSS
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 latest GPS Interface Specification (IS-GPS-200 *)
  • Incorporate DHS Best Practices (Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure *)

* Documents available on www.gps.gov

Protect GPS and Critical Infrastructure that Relies on GPS
Thank You

Stay in touch: [www.gps.gov](http://www.gps.gov)
- “GPS Bulletin” published by NCO
- Anyone can subscribe or get back issues

Contact Information:
National Coordination Office for Space-Based PNT
1401 Constitution Ave, NW – Room 2518
Washington, DC 20230
Phone: (202) 482-5809
[www.gps.gov](http://www.gps.gov)

GPS: Accessible, Accurate, Interoperable