



**SPACE-BASED POSITIONING
NAVIGATION & TIMING**
NATIONAL COORDINATION OFFICE

PNT Resilience

PNT Advisory Board

28 June 2017

**Harold W. Martin III, Director National Coordination Office
United States of America**



U.S. National Space Policy

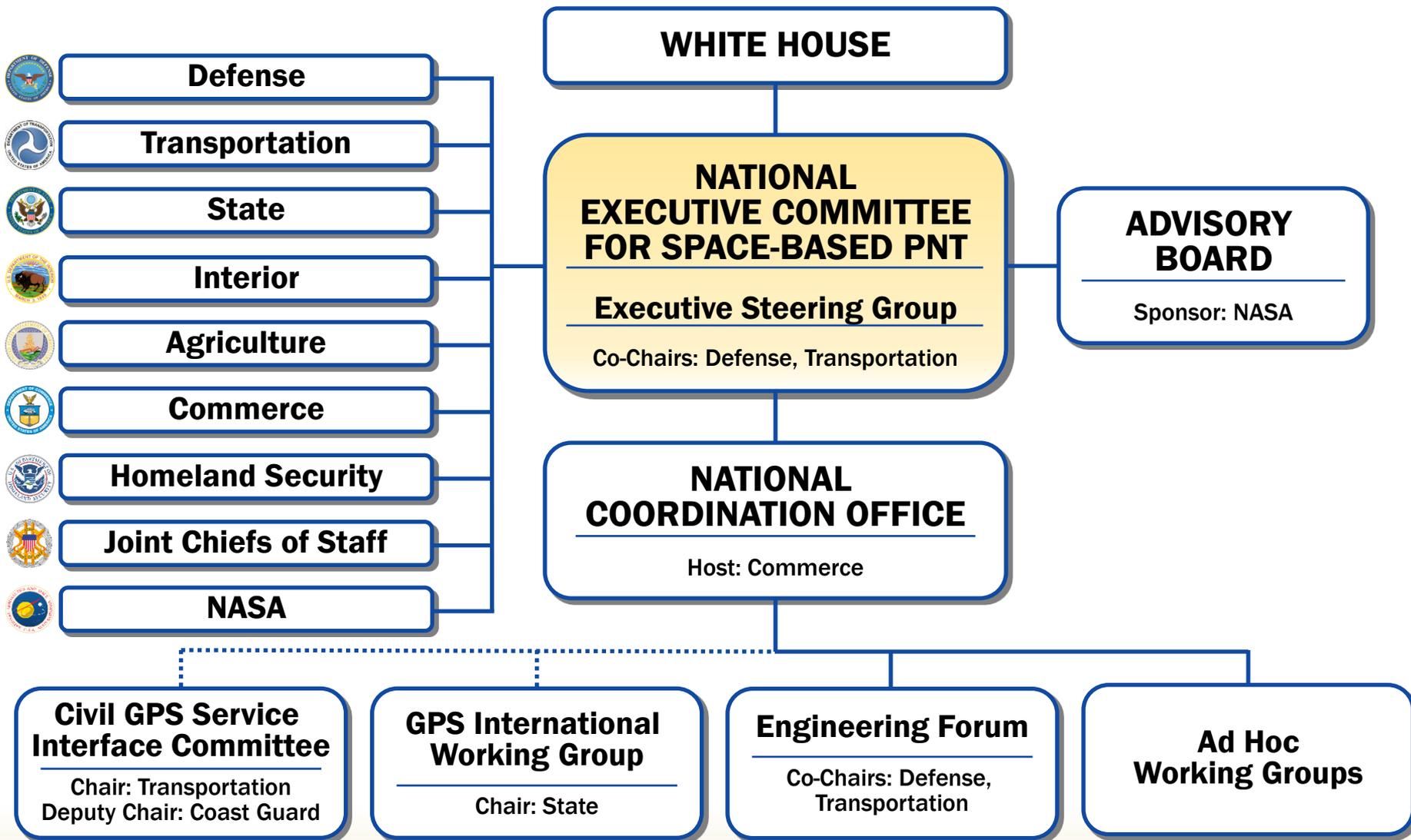


Space-Based PNT Guideline: Maintain leadership in the service, provision, and use of GNSS

- **Provide continuous worldwide access to GPS for peaceful uses, free of direct user charges**
- **Engage with foreign GNSS providers on compatibility, interoperability, transparency, and market access**
- **Operate and maintain GPS constellation to satisfy civil and national security needs**
 - Foreign PNT may be used to strengthen resiliency
- **Invest in domestic capabilities and support international activities to detect, mitigate, and increase resiliency to harmful interference**



National Space-Based PNT Organization





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 America's Critical Infrastructure
that Relies on GPS***



GPS Cyber Challenges



- **GPS receivers across the U.S. Critical Infrastructure require greater cyber resilience**
- **Interference, jamming, and spoofing challenge competence of GPS receivers and associated PNT equipment and supported systems**
 - **Measurement spoofing: introduces RF waveforms that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change.**
 - **Data spoofing: introduces incorrect digital data to the target receiver for its use in processing of signals and the calculation of PNT.**
- **Awareness regarding security and robustness of GPS and other PNT technologies needs improvement**
- **Mission critical systems and applications may be affected by the loss or manipulation of civil GPS signals**

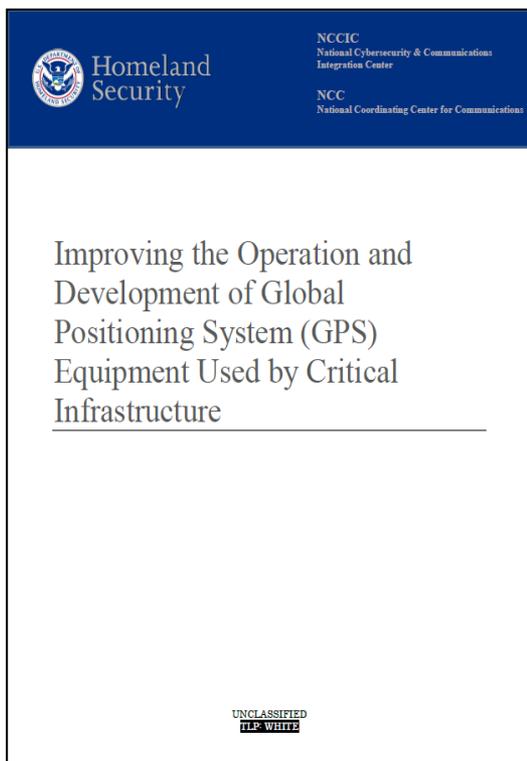


Mitigations



Best Practices:

- U.S. has released several Best Practices Documents



- Latest version (Jan 17): ***“Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure”*** (www.gps.gov)
 - Installation and Operation Strategies for Owners, Operators and Installers
 - Development Strategies for Manufacturers
 - Research Opportunities



Governance



Presidential Executive Order:

- **May 11, 2017 - Presidential Executive Order 13800, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Find the full document at: www.whitehouse.gov**
 - Cybersecurity of Federal Networks
 - Cybersecurity of Critical Infrastructure
 - Cybersecurity for the Nation
- **We need your help in protecting our systems and architectures...**
- **Its time to invest in protecting our GPS...**

“... known, but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies.”

EO 13800, May 2017



Thank You

Stay in touch: www.gps.gov

- “GPS Bulletin” published by NCO
- Anyone can subscribe or get back issues

GPS BULLETIN

Information for Policymakers from the National Coordination Office for Space-Based Positioning, Navigation, and Timing (PNT)

March 29, 2017

Update on Fiscal Year 2017 GPS Appropriations

On March 9, the House passed H.R. 1301, the revised Department of Defense appropriations bill. The measure would increase overall FY 2017 funding for the GPS program above President Obama's request.

Program Line Item	President's Request	H.R. 1301
Space Procurement: GPS III Satellites	\$34.059M	\$34.059M
Development: GPS III Satellites	\$141.888M	\$171.888M
Development: Next Generation Operational Control System (OCX)	\$393.268M	\$393.268M
Development: Military GPS User Equipment (MGUE)	\$278.147M	\$309.047M
TOTAL	\$847.362M	\$908.032M

[View full details at GPS.gov](#)

GPS Backup Discussed at Senate Hearing

At a March 22 hearing held by the Senate Subcommittee on Oceans, Atmosphere, Fisheries, & Coast Guard (OAFRCG) on the State of the Coast Guard, the Coast Guard Commandant responded to questions regarding a GPS backup.

[View hearing information at senate.gov](#)
(The discussion on GPS backup begins at 1:22:09 in the video)

GPS Act Reintroduced

In February, Sen. Ron Wyden (D-OR) and Rep. Jason Chaffetz (R-UT) reintroduced the Geolocation Privacy and Surveillance Act ("GPS Act," S. 395 and H.R. 1062). The legislation seeks to provide clarity for government agencies, commercial service providers, and the public regarding the legal procedures and protections that apply to electronic devices that can be used to

Contact Information:

National Coordination Office for Space-Based PNT
1401 Constitution Ave, NW – Room 2518
Washington, DC 20230
Phone: (202) 482-5809