SPACE-BASED POSITIONING
NAVIGATION & TIMING
NATIONAL COORDINATION OFFICE

Policy Update

National Space-Based PNT Advisory Board
Cocoa Beach, Florida

20 November 2019

Harold W. Martin III
Director
National Coordination Office

U.S. Policy

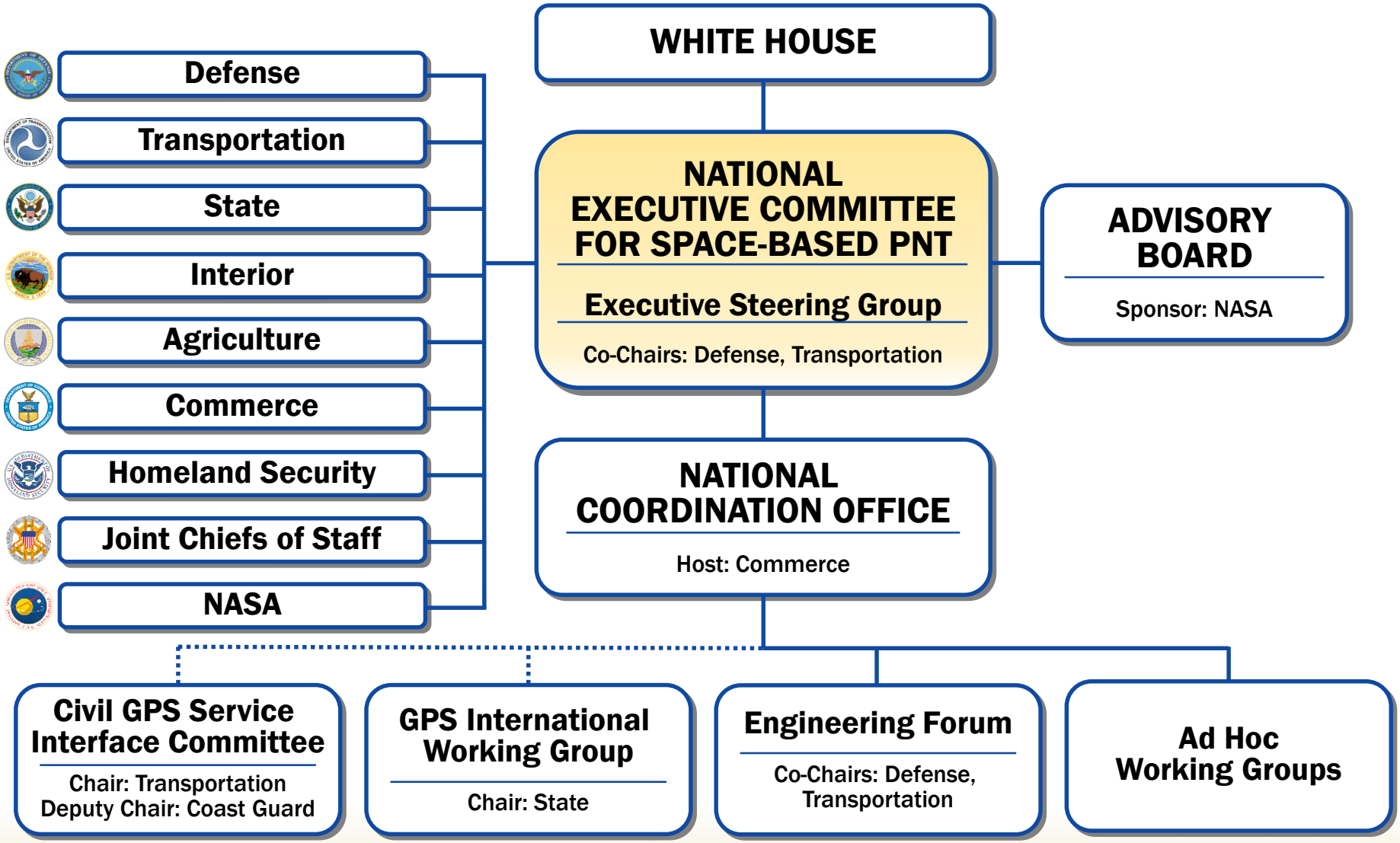
The U.S. must maintain its leadership in the service, provision, and use of Global Navigation Satellite Systems (GNSS)

- 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

U.S. Policy

- NSPD-39, the Space-Based Positioning, Navigation, and Timing Policy from 2004, is in the process of being updated by the National Space Council
- Remarks by DOT General Counsel at the 6th Meeting of the National Space Council:
  - Under National Security Presidential Directive 39, issued in December 2004, the United States is committed to developing, maintaining and a modernizing the global positioning system, or GPS, and other satellite-based navigation systems, including backup capability in the event of a disruption of GPS.
  - …"Working closely with the Commerce Department, NTIA, and the FCC," DOT's adjacent band compatibility study "shows we need strong, consistent policies to ensure protection for satellite-based navigation."

National Space-Based PNT Organization



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 require Cybersecurity
- U.S. Policy directs PNT resiliency (NSPD-39, PPD-4, PPD-21, EO 13800, National Cyber Strategy)

"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 latest GPS Interface Specification (IS-GPS-200K *)
  - 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

- "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

GPS: Accessible, Accurate, Interoperable