NIST Workshop Kickoff KEYNOTE

24 June 2021

Mr. Charlie Brown, DAF
U.S. Space Force Cyber Security for Space Production Corps

What is PNT?

- PNT is a combination of three distinct, constituent capabilities:
- **Positioning**, the ability to accurately and precisely determine one's location and orientation two-dimensionally (or three-dimensionally when required) referenced to a standard geodetic system (such as World Geodetic System 1984, or WGS84);
- **Navigation**, the ability to determine current and desired position (relative or absolute) and apply corrections to course, orientation, and speed to attain a desired position anywhere around the world, from sub-surface to surface and from surface to space; and
- **Timing**, the ability to acquire and maintain accurate and precise time from a standard (Coordinated Universal Time, or UTC), anywhere in the world and within user-defined timeliness parameters. Timing also includes time transfer.
- When PNT is used in combination with map data and other information (weather or traffic data, for instance) the result is the most popular and recognizable service--the modern navigation system better known as the Global Positioning System (GPS)

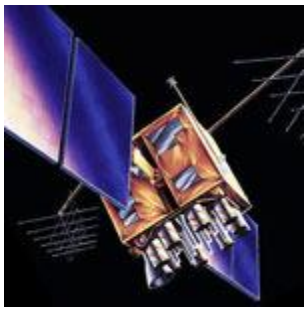
Source: What is Positioning, Navigation and Timing (PNT)? | US Department of Transportation

PNT Services

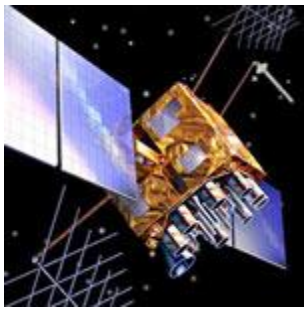
- In accordance with Executive Order 13905, the Air Force's Space and Missile Systems Center (SMC) is working to ensure Position, Navigation and Timing (PNT) services provided by GPS has resiliency and reliable as the nation's critical infrastructure depends on it
- Under this Executive Order, Department of Commerce, Department of Defense and other federal agencies will work to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of the nation's critical economic infrastructure.
- SMC is seeking to leverage the existing National Institute of Standards and Technology (NIST) Cybersecurity expertise and techniques to increase GPS resiliency.
  - In particular, SMC is seeking diversity of perspective especially with regards to our industry partners on how to secure GPS ground control segment

GPS – Three Segments Overview

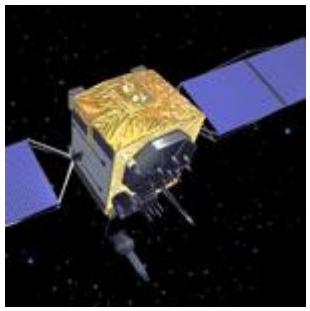
Space Segment



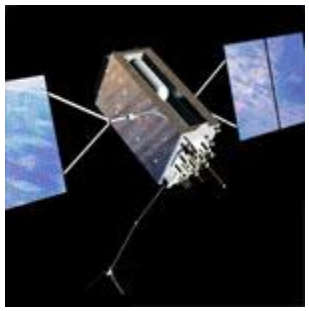
GPS IIR



GPS IIR-M



GPS IIF



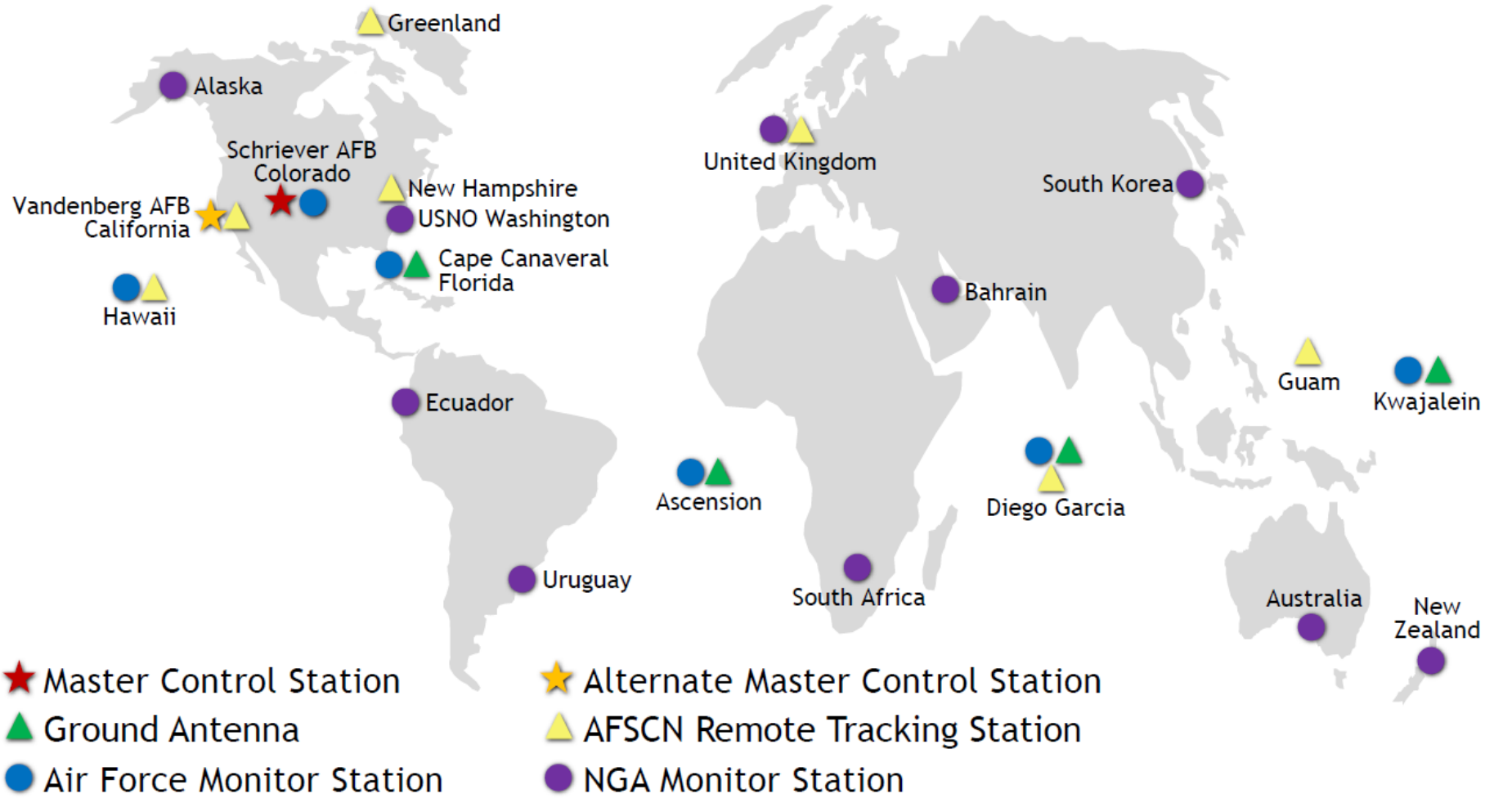
GPS III

Control Segment

User Segment

Source: GPS.gov

GPS – Control Segment

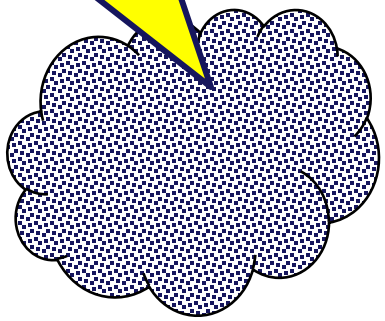


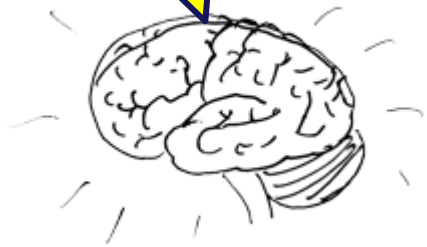
Ground Segment Cyber Challenges

Control Inputs

Isolate Functions

Protect Link





Inputs

Control Station

Ground Antennas

Prevent Disruption

Satellite Operations

Payload Operations

Maintain Autonomy

Industry Questions

- **What are the most pressing cybersecurity challenges satellite operators face today with regards to their ground segment?**
- **What are the leading practices employed to mitigate these challenges?**
- **What are the biggest cybersecurity challenges/threats looming over the horizon for ground segments?**
- **What reasonable/doable future ground segment cybersecurity initiatives do you believe industry should undertake?**