DHS SCIENCE AND TECHNOLOGY

A Holistic Approach to PNT Resilience

Orolia Coffee Talk

March 24, 2021

Ernest Wong

Technical Manager
Technology Centers Division
Science and Technology Directorate

Homeland Security
Science and Technology

What is “Responsible Use of PNT”?

- E.O.13905 Definition: “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.”

- PNT Profile serves as risk assessment and management tool.

- Objective of “Responsible Use of PNT” is to assess and limit the impacts of PNT disruptions to critical applications and operations.

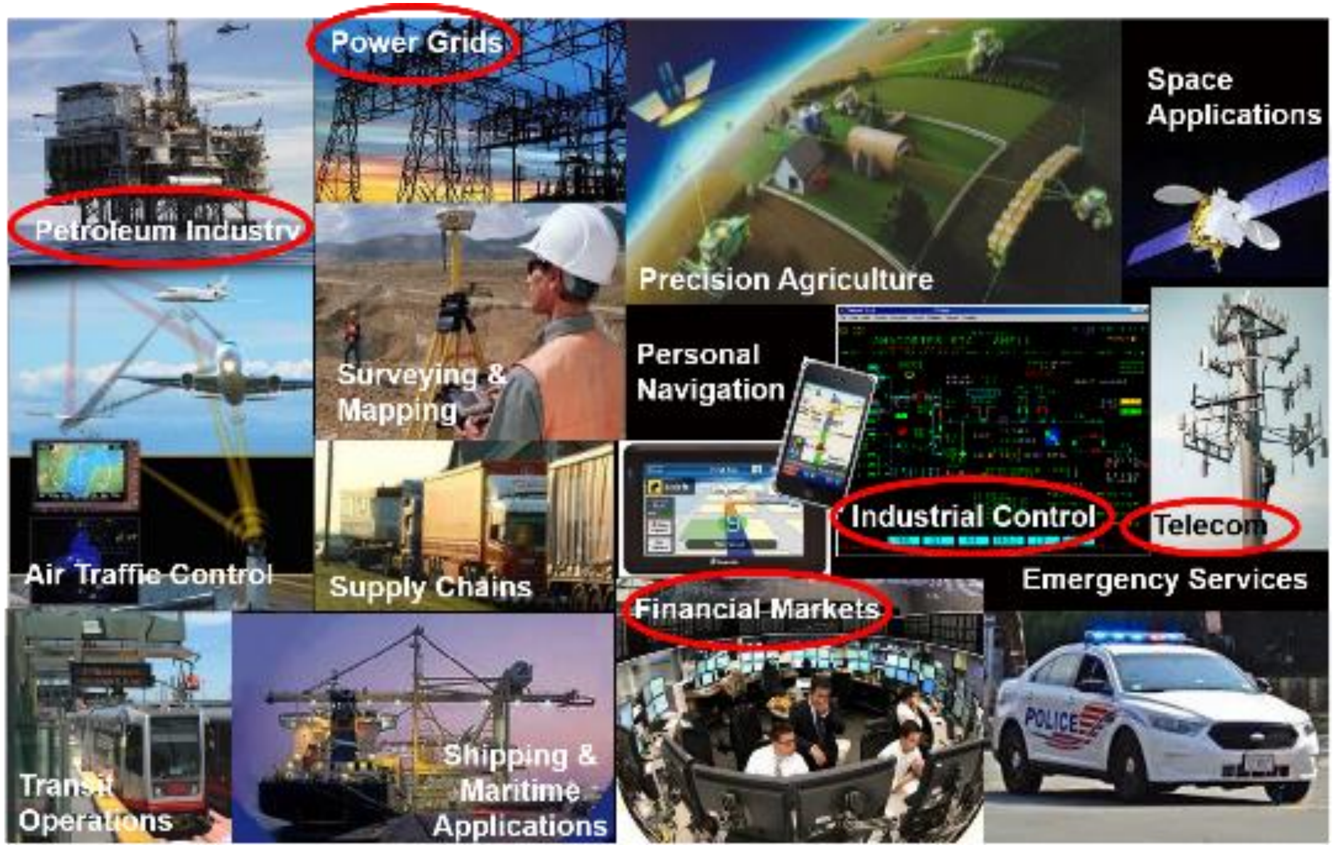
- How to address critical applications and use cases with significant PNT dependencies? Need an approach for building PNT resilience to limit impacts of disruptions.

Presentation Outline

- **GPS Background Review**
- **Re-Framing the Problem**
- **Holistic Approach to PNT Resilience**
- **Key DHS R&D Activities**
  - Conformance Framework
  - Reference Architecture
  - Spoofing Detection Toolkits
- **Conformance Framework vs. Responsible Use of PNT**
  - Risk at the receiver level vs. system level usage
  - Role of Vulnerability Test Plan

GPS: Much more than just a navigation tool

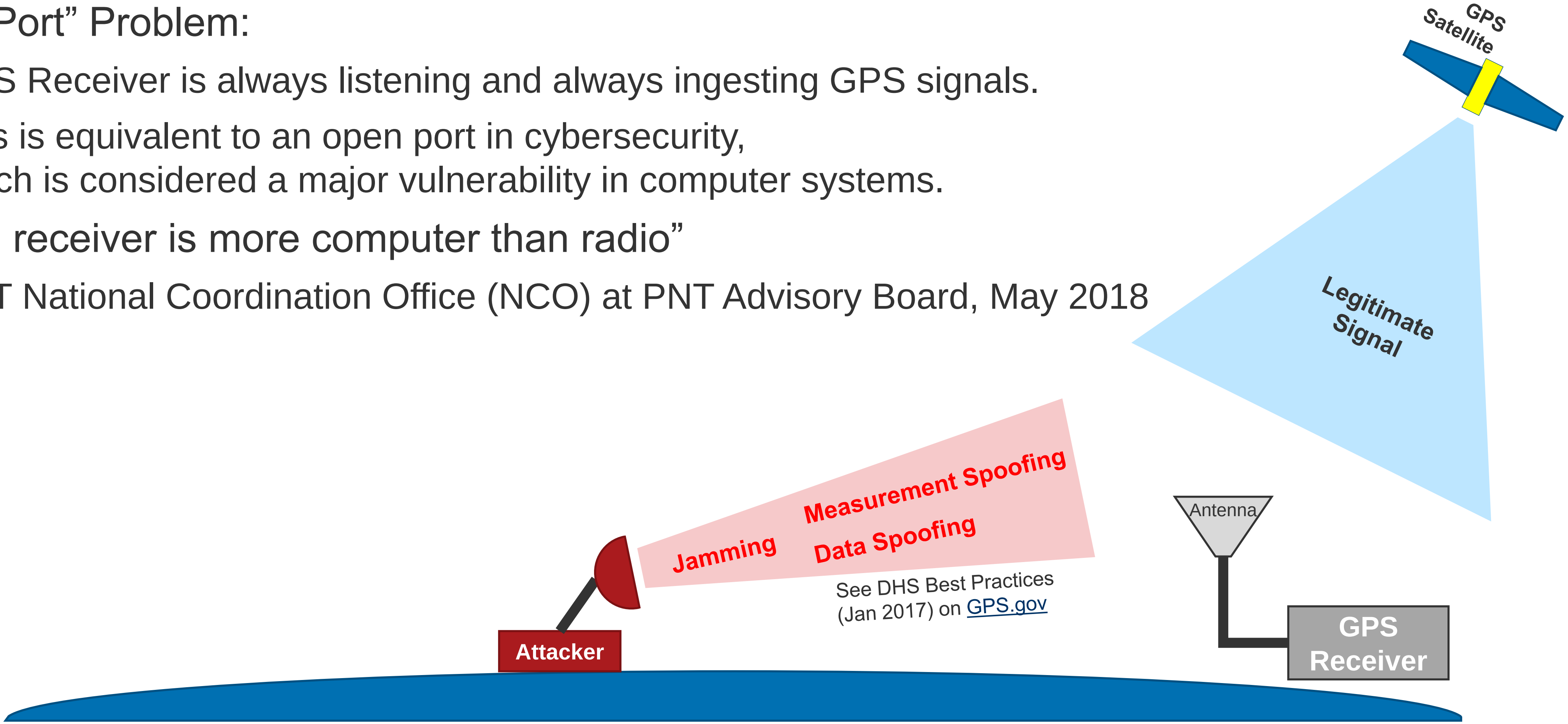
- GPS as an “invisible utility” enabling critical infrastructure sectors:



U.S. CUSTOMS AND BORDER PROTECTION
U.S. DEPARTMENT OF HOMELAND SECURITY

Re-Framing the Problem (1): Open Ports

- "Open Port" Problem:
  - GPS Receiver is always listening and always ingesting GPS signals.
  - This is equivalent to an open port in cybersecurity,
    which is considered a major vulnerability in computer systems.
- "A GPS receiver is more computer than radio"
  - PNT National Coordination Office (NCO) at PNT Advisory Board, May 2018



See DHS Best Practices (Jan 2017) on GPS.gov

Re-Framing the Problem (2): Trends & Risks

- Based on industry trends, the future of PNT involves a multitude of signals.
- However, every PNT source is an attack surface.

Past

1 open port

Present & Future

+Non-GNSS
Sources

Many open ports

A Holistic Approach for PNT Resilience

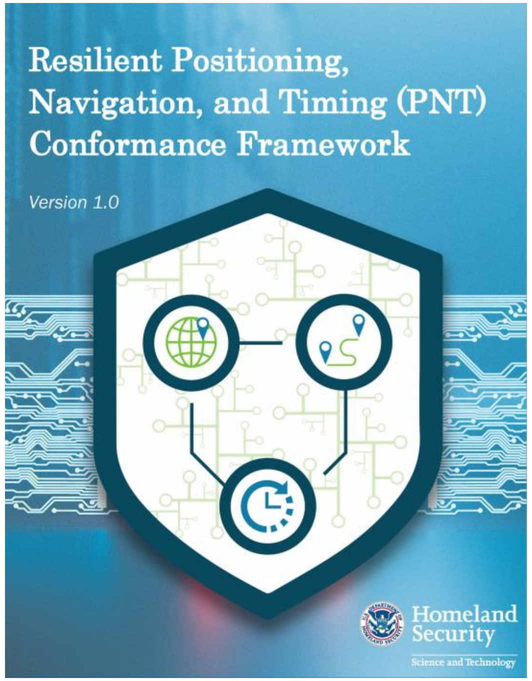
- Assumptions:
  - With the future of PNT involving a multitude of PNT sources, every PNT source should be treated as an attack surface.
  - However, it is cost prohibitive, slow, and reactive to conduct equipment vulnerability assessments against every new PNT source, develop mitigations, deploy/transition them, and wait for new equipment acquisition cycles. Also, this is not scalable.

- Requirements for NextGen Resilient PNT:
  - Assume systems will be attacked and design them so they can withstand and recover.
  - Futureproof, proactive, and agnostic approach to threats (versus reactive antivirus-like detection).
  - Cybersecurity approach of not assuming trust.

- Architecture Elements:
  - Minimized and harden attack surfaces
  - Distinction between trusted vs. untrusted components and data
  - Component isolation and secure interfaces
  - Protected internal trusted states
  - Controlled intake of untrusted external data
  - Recovery capability from any attack

2021 DHS Products for PNT Resilience

- **Resilient PNT Conformance Framework**
  - Outcome-based and solution agnostic framework for defining expected behaviors from resilient PNT equipment across four levels of resilience. Defined behaviors for four levels of resilience.
  - Developed in collaboration with industry and federal interagency partners. Planned transition to IEEE.
  - Abstract incorporation of some key concepts from prior slide.
- **Reference Architecture**
  - Complements Conformance Framework by providing concrete examples implementing all resilience concepts described.
- **PNT Integrity Library**
  - End-to-end GPS spoofing detection capability. Enhancement in near-term.
  - Modular Application Programming Interface (API).
  - Open source and released on CISA GitHub.



Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework

Version 1.0

Homeland Security

Science and Technology

Next Steps

- **Standards Development**
  - Planning transition of Conformance Framework to IEEE. Project Authorization Request (PAR) submitted to IEEE in February.
  - If approved, IEEE will need working group members for this activity.
  - Decision expected in late April.

- **Reference Architecture**
  - Companion document to the Conformance Framework that fleshes out resilience concepts further.
  - Planned for presentation in Fall 2021.

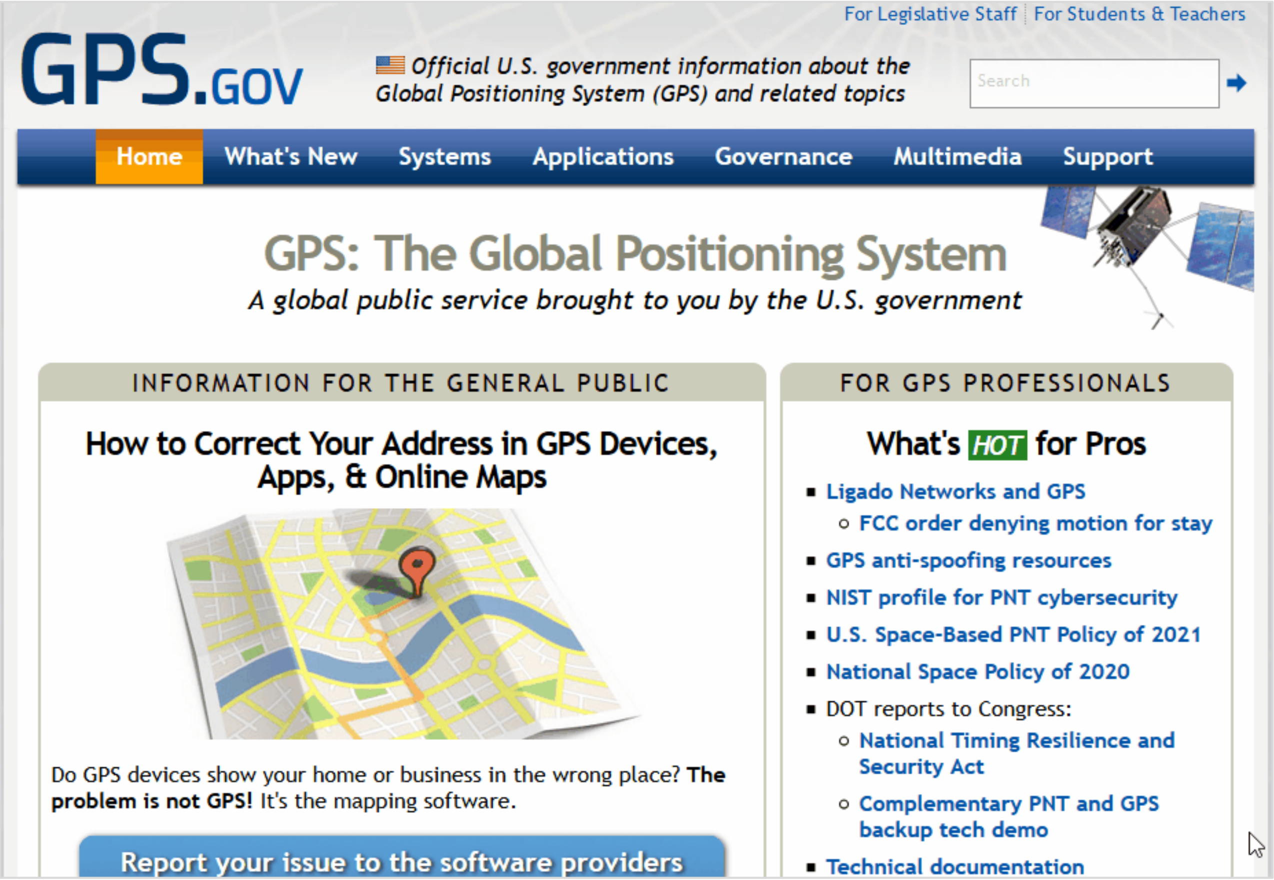
Responsible Use of PNT & Resilient PNT Conformance Framework

- **Resilient PNT Conformance Framework**
  - Focus: Systems that deliver PNT data.
  - Purpose: Facilitate development and adoption of resilient end-user systems that output PNT data.
- **EO13905: Responsible Use of PNT**
  - Focus: Entire PNT ecosystem, including downstream applications that consume PNT data.
  - Purpose: Risk-based approach to assessing and limiting the impact of PNT dependencies to critical operations.

- **PNT Executive Order: Vulnerability Test Plans**
  - Timeframe: Later this year and continuing for next few years.
  - DHS will work with critical infrastructure operators to assess vulnerability to PNT disruption or corruption.
  - Results will inform updates to foundational profile and/or development of tailored profiles.

Resource Links

- GPS.gov Resilience Repository
  - https://www.gps.gov/resilience/
- DHS Resilient PNT Conformance Framework
  - https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework
- PNT Integrity Library
  - https://github.com/cisagov/PNT-Integrity
- Epsilon Algorithms
  - https://github.com/cisagov/Epsilon
- DHS S&T PNT Program
  - https://www.dhs.gov/science-and-technology/pnt-program
- DHS CISA PNT Program Management Office
  - https://www.cisa.gov/pnt



Official U.S. government information about the Global Positioning System (GPS) and related topics

GPS: The Global Positioning System

A global public service brought to you by the U.S. government

INFORMATION FOR THE GENERAL PUBLIC

How to Correct Your Address in GPS Devices, Apps, & Online Maps

Do GPS devices show your home or business in the wrong place? **The problem is not GPS!** It's the mapping software.

Report your issue to the software providers

FOR GPS PROFESSIONALS

What's HOT for Pros

- Ligado Networks and GPS
  - FCC order denying motion for stay
- GPS anti-spoofing resources
- NIST profile for PNT cybersecurity
- U.S. Space-Based PNT Policy of 2021
- National Space Policy of 2020
- DOT reports to Congress:
  - National Timing Resilience and Security Act
  - Complementary PNT and GPS backup tech demo
- Technical documentation

Homeland Security

Science and Technology

DIVERSE PERSPECTIVES + SHARED GOALS = POWERFUL SOLUTIONS