



# DHS SCIENCE AND TECHNOLOGY

## Resilient PNT Reference Architecture:

Applying Cybersecurity Concepts to PNT Resilience

PNT Advisory Board

**May 4, 2022**



**Homeland  
Security**

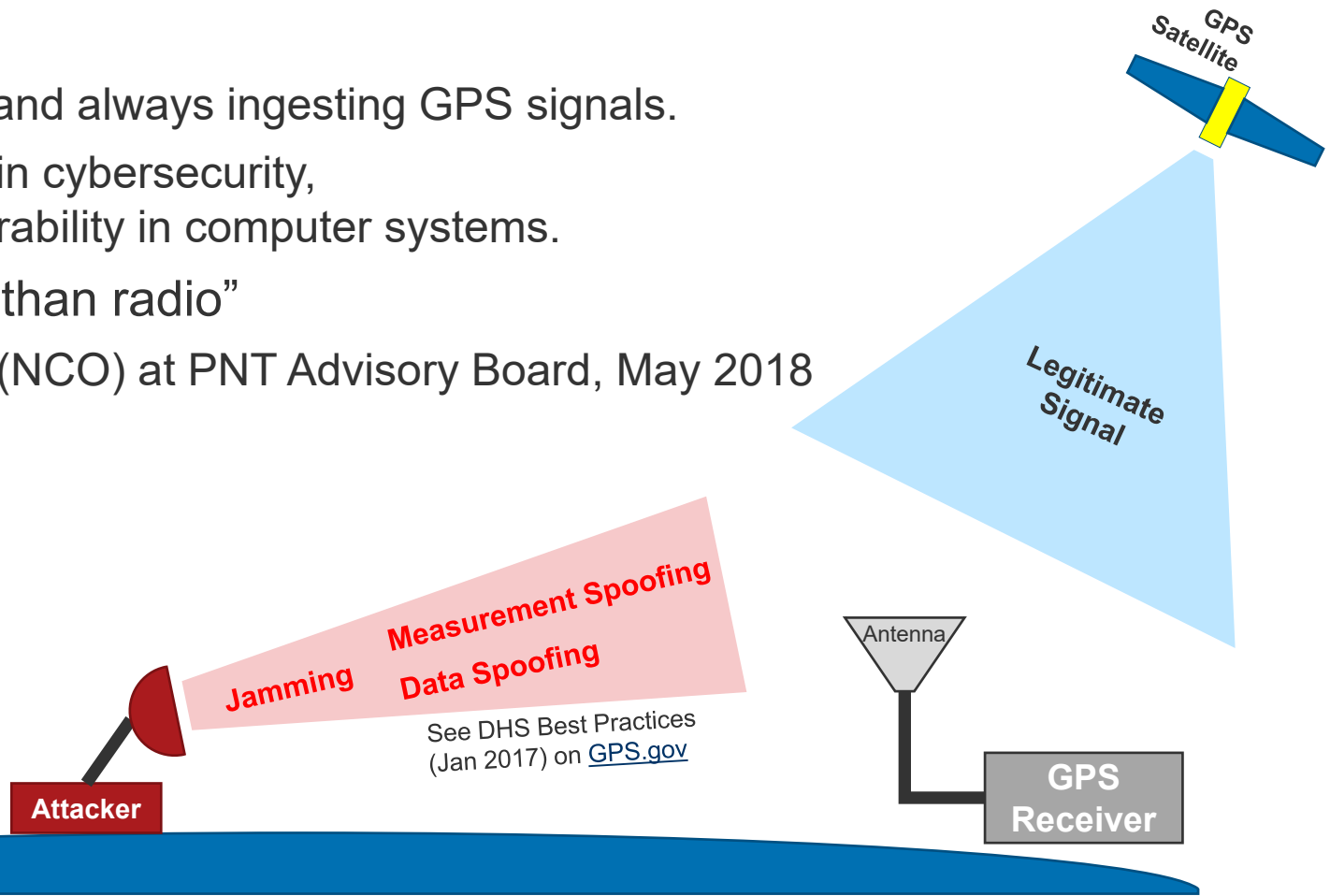
Science and Technology

**Ernest Wong**

Technical Manager, PNT Technical Lead  
Technology Centers Division  
Science and Technology Directorate

# Cybersecurity Lens: 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



# Cybersecurity Lens: Attack Surfaces

- 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

# Resilient PNT Reference Architecture

## ■ Purpose

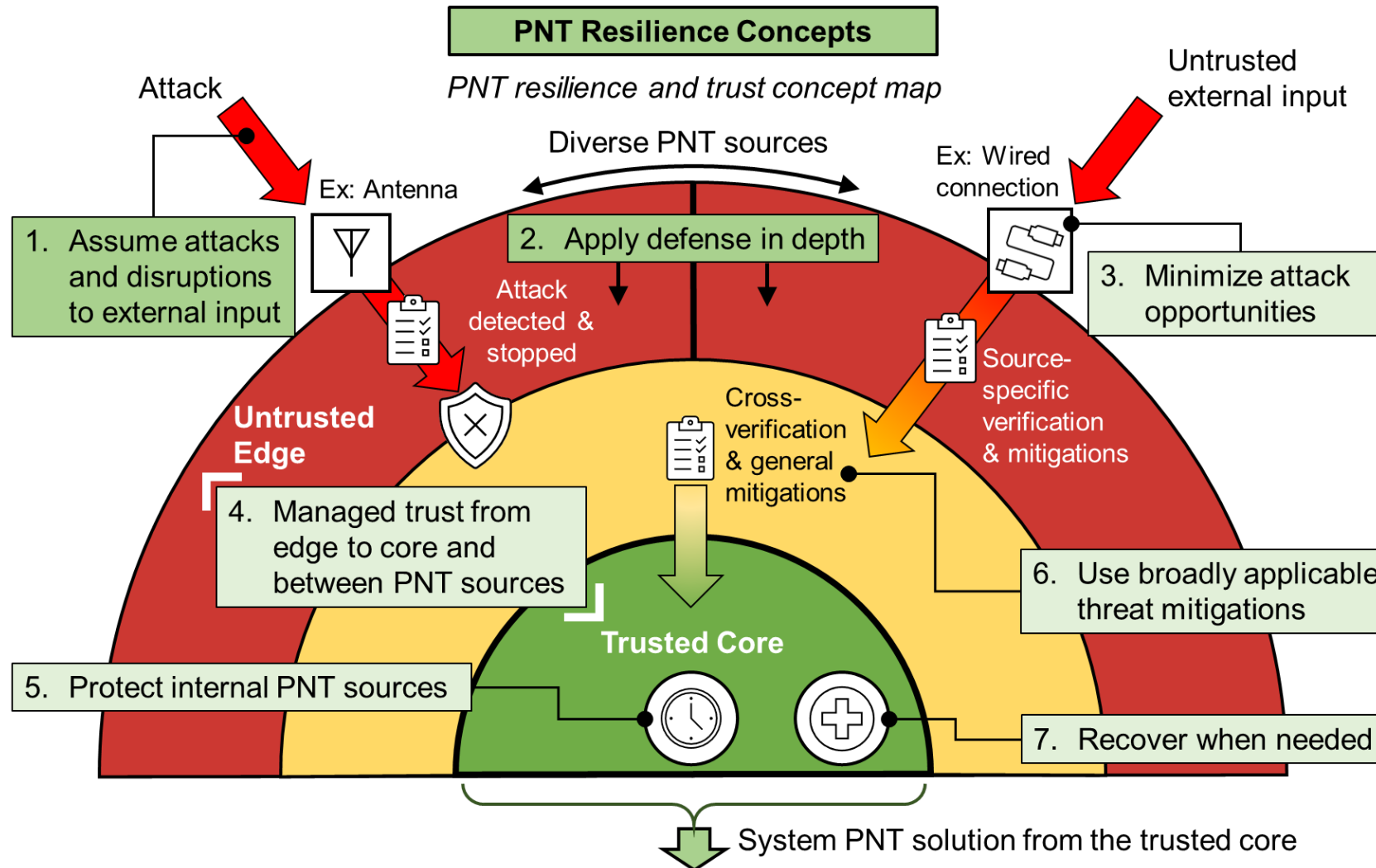
1. Follow-on to Conformance Framework that provides concrete implementation examples. The CF was non-prescriptive in nature. The RA describe more clearly what was intended by the CF.
2. Introduces how to implement modern cybersecurity principles (including Zero Trust Architectures) into PNT resilience.

Applying these concepts in the design of NextGen Resilient PNT systems will enable them to be resilient against both current and future threats, through containing the impact of attacks and disrupting exploit chains.

# What is Zero Trust?

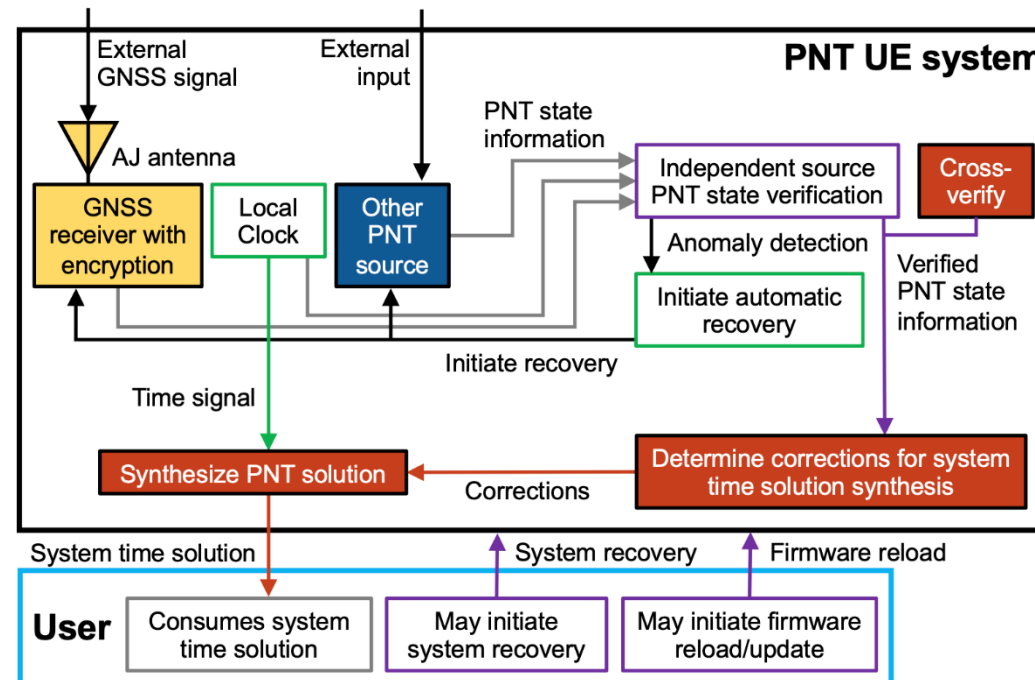
- **Objective of ZTA:** Contain and limit the impact of successful attacks and intrusions.
- **Key Requirements for Applying to PNT**
  - Verification
  - Component Isolation
- **Trusted Core:** If isolated properly, is inherently trusted as it does not require external input.
- **Untrusted Edge:** Inherently untrusted as it sits at the edge of the system and is an attack surface.
- **Implementation:** Ideal case is full isolation in a CF Level 4 receiver. But can scale down the concepts to lower levels.

# Applying Zero Trust Concepts to PNT



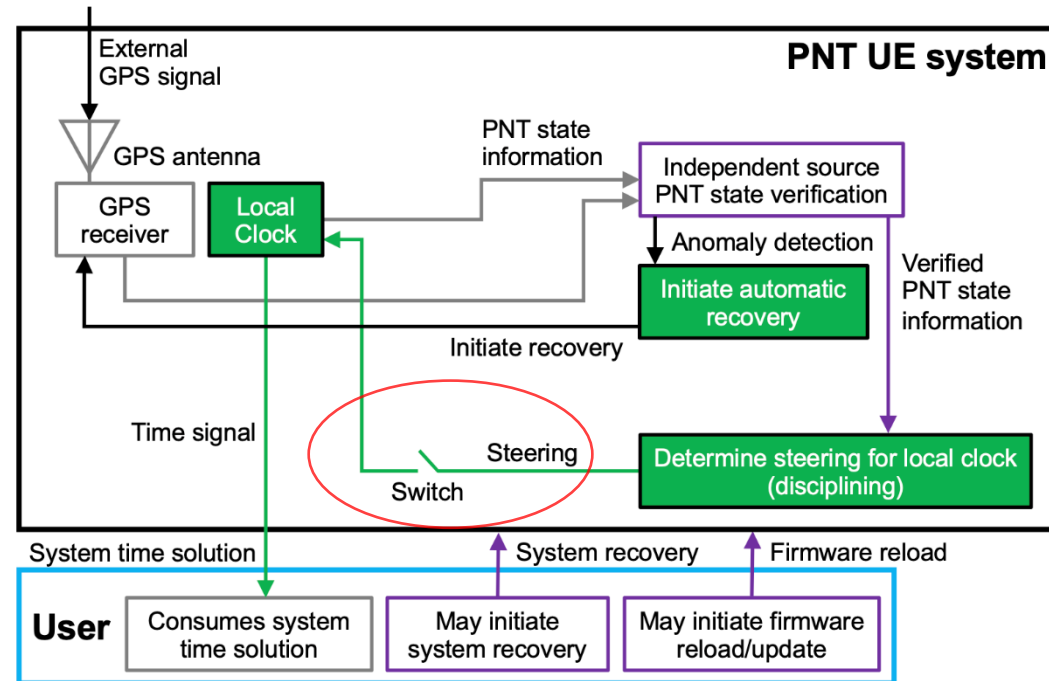
# Level 3-4 Implementation Example

- Internal clock = primary source (b/c it's trusted the most—vs. GNSS source on the untrusted edge)
- Internal clock fully isolated. Corrections applied at solution synthesizer.



# Level 2 Implementation Example

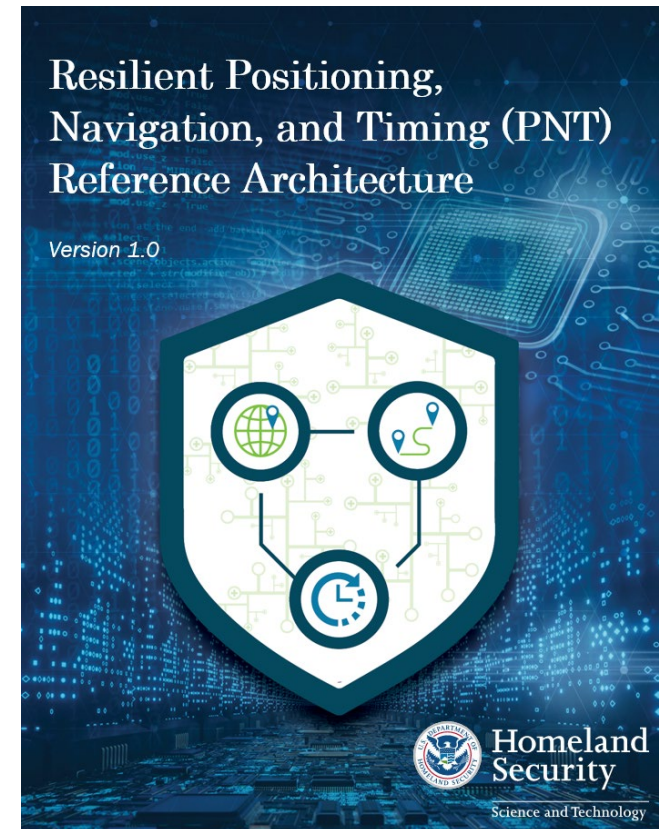
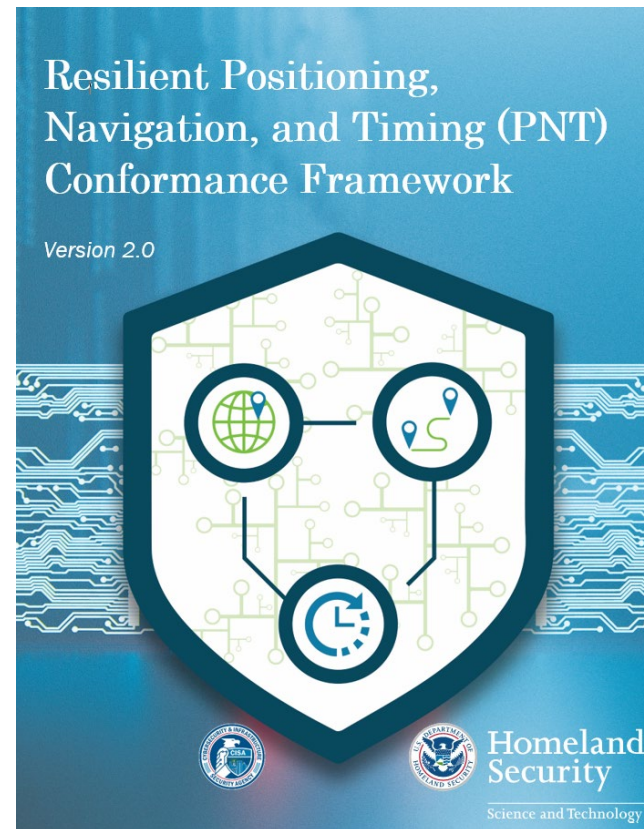
- Internal clock still primary source (b/c of trusted core vs. untrusted edge)
- Less isolation but can achieve some degree of it through the **FLIP** method (limit exposure to attack surface).





# Upcoming Publications

- Planned publication in next 1-2 months:
  - Resilient PNT Conformance Framework v2.0
  - Resilient PNT Reference Architecture 1.0
- Will be posted to S&T website and GPS.gov



# 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>

The screenshot shows the GPS.gov website interface. At the top right, there are language options: English, español, français, 中文, and عربي. Below these are links for 'For Legislative Staff' and 'For Students & Teachers'. The main header features the 'GPS.gov' logo and the text 'Official U.S. government information about the Global Positioning System (GPS) and related topics'. A search bar is located to the right of the logo. The navigation menu includes 'Home', 'What's New', 'Systems', 'Applications', 'Governance', 'Multimedia', and 'Support'. The main content area displays 'GPS: The Global Positioning System' with the tagline 'A global public service brought to you by the U.S. government'. Below this, there are two tabs: 'INFORMATION FOR THE GENERAL PUBLIC' and 'FOR GPS PROFESSIONALS'. A green arrow points from the 'FOR GPS PROFESSIONALS' tab to a specific link in the lower right corner of the page, which is circled in red. The link is 'Resilience Through Responsible Use of PNT' with a right-pointing arrow. Below this link is the text 'Information and resources for improving positioning, navigation, and timing resilience, especially in critical infrastructure'. At the bottom of the page, there is a button that says 'Report/Lookup GPS Service Disruptions' with a right-pointing arrow.



# Homeland Security

---

Science and Technology

**DIVERSE PERSPECTIVES + SHARED GOALS = POWERFUL SOLUTIONS**