CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

OVER DEPENDENCE ON GPS

WSTS CONFERENCE
MAY 2022

Jim Platt/NRMC
May 9, 2022

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

National Risk Management Center

The NRMC is a planning, analysis, and collaboration center. CISA coordinates with the critical infrastructure community to identify; analyze; prioritize; and manage risks to National Critical Functions, which are vital to the United States.

MISSION

Collaborate with partners to analyze and reduce risks to National Critical Functions

VISION

A secure tomorrow where strategic risks to critical infrastructure are mitigated to enhance the Nation’s resilience

Position, Navigation, and Timing

On a daily basis, critical infrastructure depends on the Positioning, Navigation and Timing services provided by GPS. DHS is working to ensure critical infrastructure systems are designed to manage risks associated with the use, and potential overdependence, on the GPS signal

On February 12, 2020, the Executive Order (E.O.) 13905 on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services was signed. The goal of the E.O. was to identify and promote the responsible use of PNT services by the Federal Government and critical infrastructure owners and operators

National Critical Functions Set

CONNECT

- Operate Core Network
- Provide Cable Access Network Services
- Provide Internet Based Content, Information, and Communication Services
- Provide Internet Routing, Access and Connection Services
- Provide Positioning, Navigation, and Timing Services
- Provide Radio Broadcast Access Network Services
- Provide Satellite Access Network Services
- Provide Wireless Access Network Services
- Provide Wireline Access Network Services

DISTRIBUTE

- Distribute Electricity
- Maintain Supply Chains
- Transmit Electricity
- Transport Cargo and Passengers by Air
- Transport Cargo and Passengers by Rail
- Transport Cargo and Passengers by Road
- Transport Cargo and Passengers by Vessel
- Transport Materials by Pipeline
- Transport Passengers by Mass Transit

MANAGE

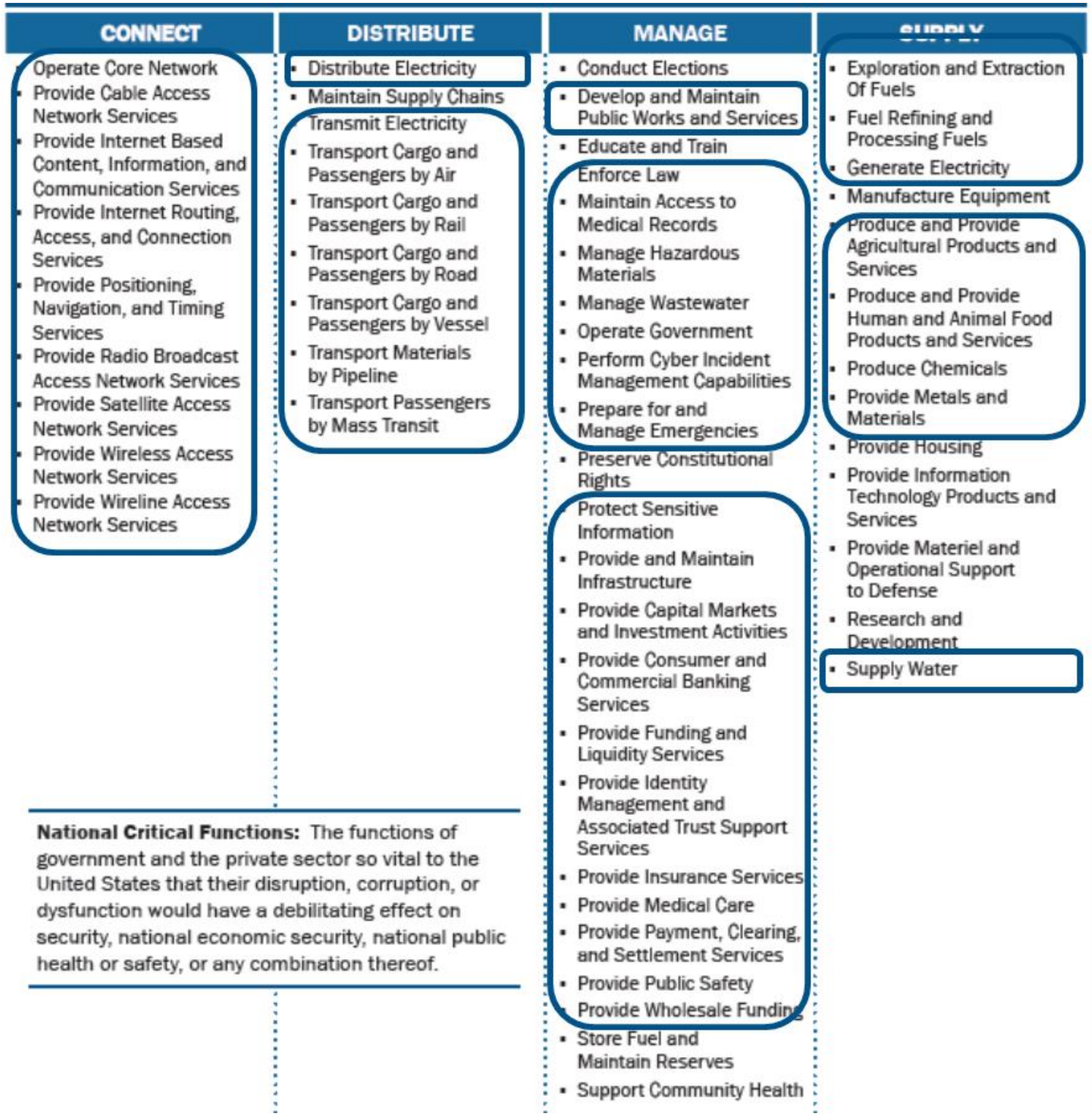
- Conduct Elections
- Develop and Maintain Public Works and Services
- Educate and Train
- Enforce Law
- Maintain Access to Medical Records
- Manage Hazardous Materials
- Manage Wastewater
- Operate Government
- Perform Cyber Incident Management Capabilities
- Prepare For and Manage Emergencies
- Preserve Constitutional Rights
- Protect Sensitive Information
- Provide and Maintain Infrastructure
- Provide Capital Markets and Investment Activities
- Provide Consumer and Commercial Banking Services
- Provide Funding and Liquidity Services
- Provide Identity Management and Associated Trust Support Services
- Provide Insurance Services
- Provide Medical Care
- Provide Payment, Clearing, and Settlement Services
- Provide Public Safety
- Provide Wholesale Funding
- Store Fuel and Maintain Reserves
- Support Community Health

SUPPLY

- Exploration and Extraction Of Fuels
- Fuel Refining and Processing Fuels
- Generate Electricity
- Manufacture Equipment
- Produce and Provide Agricultural Products and Services
- Produce and Provide Human and Animal Food Products and Services
- Produce Chemicals
- Provide Metals and Materials
- Provide Housing
- Provide Information Technology Products and Services
- Provide Materiel and Operational Support to Defense
- Research and Development
- Supply Water

Understanding PNT as a National Critical Function

- Providing PNT is National Critical Function that enables or enhances many other NCFs.
- Loss of GPS has been estimated at $1 billion/day due to either the loss or degradation of the NCFs highlighted to the right.
- DHS encourages the "Responsible use of PNT" in accordance with Executive Order 13905 to improve the security and resilience of supported NCFs.
- Example: April 6, 2019 - Global impacts from a GPS System design limitation known as a "week number rollover."
  - Many transoceanic flights grounded
  - Some communications systems disrupted for a week
  - Loss of control for some traffic control devices



CONNECT

- Operate Core Network
- Provide Cable Access Network Services
- Provide Internet Based Content, Information, and Communication Services
- Provide Internet Routing, Access, and Connection Services
- Provide Positioning, Navigation, and Timing Services
- Provide Radio Broadcast Access Network Services
- Provide Satellite Access Network Services
- Provide Wireless Access Network Services
- Provide Wireline Access Network Services

DISTRIBUTE

- Distribute Electricity
- Maintain Supply Chains
- Transmit Electricity
- Transport Cargo and Passengers by Air
- Transport Cargo and Passengers by Rail
- Transport Cargo and Passengers by Road
- Transport Cargo and Passengers by Vessel
- Transport Materials by Pipeline
- Transport Passengers by Mass Transit

National Critical Functions: The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

MANAGE

- Conduct Elections
- Develop and Maintain Public Works and Services
- Educate and Train
- Enforce Law
- Maintain Access to Medical Records
- Manage Hazardous Materials
- Manage Wastewater
- Operate Government
- Perform Cyber Incident Management Capabilities
- Prepare for and Manage Emergencies
- Preserve Constitutional Rights
- Protect Sensitive Information
- Provide and Maintain Infrastructure
- Provide Capital Markets and Investment Activities
- Provide Consumer and Commercial Banking Services
- Provide Funding and Liquidity Services
- Provide Identity Management and Associated Trust Support Services
- Provide Insurance Services
- Provide Medical Care
- Provide Payment, Clearing, and Settlement Services
- Provide Public Safety
- Provide Wholesale Funding
- Store Fuel and Maintain Reserves
- Support Community Health

SUPPLY

- Exploration and Extraction Of Fuels
- Fuel Refining and Processing Fuels
- Generate Electricity
- Manufacture Equipment
- Produce and Provide Agricultural Products and Services
- Produce and Provide Human and Animal Food Products and Services
- Produce Chemicals
- Provide Metals and Materials
- Provide Housing
- Provide Information Technology Products and Services
- Provide Materiel and Operational Support to Defense
- Research and Development
- Supply Water

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

DHS 2018 Report to Congress

Key Finding:

"Critical infrastructure systems that cease to operate due to GPS disruptions will do so because of design choices and other considerations—not because of a lack of available options. In other words, business decisions, the lack of a Federal mandate, and potentially an underappreciation of the risk associated with GPS dependence are factors in the lack of resilience to GPS disruption."

Coordinate implementation of requirement in Executive Order 13905 and Space Policy Directive 7

Jim Platt/NRMC
May 9, 2022

DHS Views on PNT Resilience

Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS)

National Defense Authorization Act Fiscal Year 2017 Report to Congress: PNT *Requirements, and Analysis of Alternatives*

April 8, 2020

Homeland Security

Key Recommendations

- End Users Responsible for Short Term Disruptions
- Encourage Diversity and Segmentation
- Improve the design of Critical Systems
- Focus: R&D that facilitates transition and adoption

Denver – Why this is important

Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS)

National Defense Authorization Act Fiscal Year 2017 Report to Congress: PNT *Requirements, and Analysis of Alternatives*

April 8, 2020

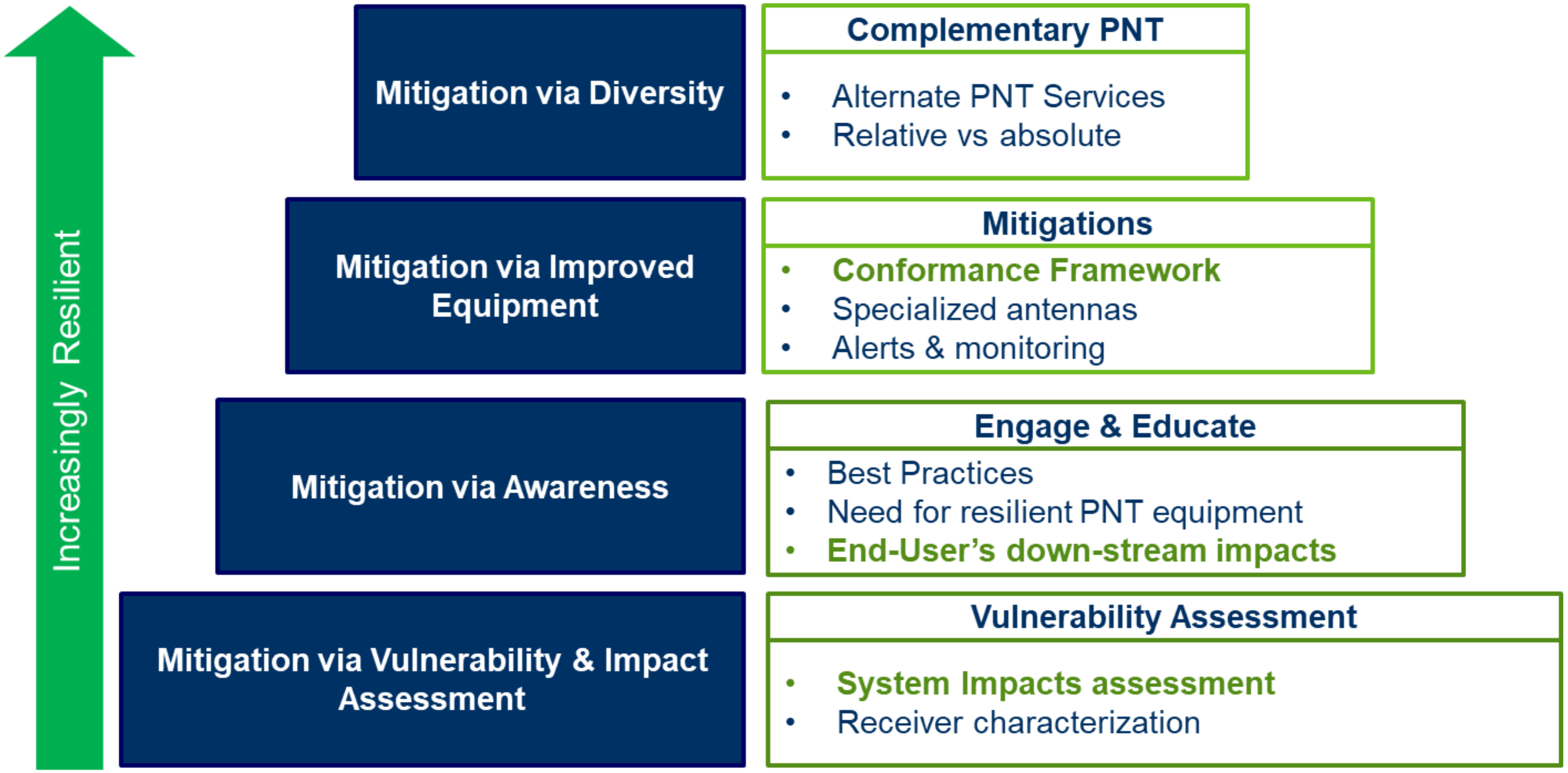
Homeland Security

Denver

- Entity A – Critical functions disrupted
- Entity B – Swapped parts to try and rectify
- Entity C – Some degradation
- Entity D – "We saw it. No operations were impacted"

PNT Strategic Overview

Holistic view with a layered approach



Increasingly Resilient

Mitigation via Diversity

Complementary PNT

- Alternate PNT Services
- Relative vs absolute

Mitigation via Improved Equipment

Mitigations

- **Conformance Framework**
- Specialized antennas
- Alerts & monitoring

Mitigation via Awareness

Engage & Educate

- Best Practices
- Need for resilient PNT equipment
- **End-User's down-stream impacts**

Mitigation via Vulnerability & Impact Assessment

Vulnerability Assessment

- **System Impacts assessment**
- Receiver characterization

It is more then just the receiver. Security and Resilience must be approached from a systems level view.

Cybersecurity View of GPS Threats

RSAConference2021
May 17 – 20 | Virtual Experience

SESSION ID: SAT-W11

Strengthening Resilience of Positioning, Navigation, and Timing Services

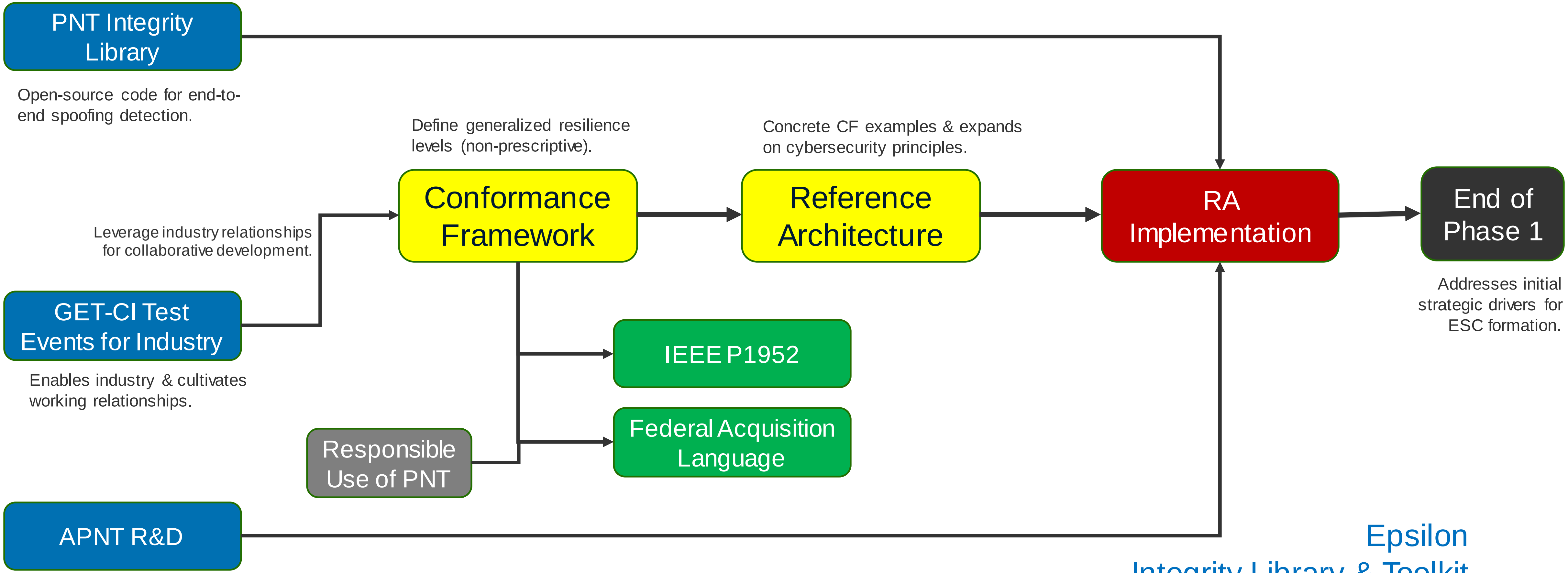
James McCarthy
Senior Security Engineer
National Cybersecurity Center of Excellence
National Institute of Standards and Technology
@NISTcyber

James Platt
Chief, Strategic Defense Initiatives
Cybersecurity & Infrastructure Security Agency
U.S. Department of Homeland Security
@CISAgov

#RSAC

Cybersecurity Threat	GPS Equivalent	Effect
Distributed Denial of Service (DDoS)	GPS Jamming	Denial of service only during attack.
Ransomware	GPS Data Spoofing (select attacks) Example: 2017 ION GNSS+	Persistent denial of service (even after attack ends).
Other Intrusions for Impact (MITRE ATT&CK Framework T1565: Data Manipulation)	GPS Spoofing	Compromises system and data integrity. Risk to operations and decision making.

S&T Vision for Holistic PNT Resilience



PNT Integrity Library

Open-source code for end-to-end spoofing detection.

Leverage industry relationships for collaborative development.

GET-CI Test Events for Industry

Enables industry & cultivates working relationships.

Define generalized resilience levels (non-prescriptive).

Conformance Framework

Concrete CF examples & expands on cybersecurity principles.

Reference Architecture

RA Implementation

End of Phase 1

Addresses initial strategic drivers for ESC formation.

IEEE P1952

Federal Acquisition Language

Responsible Use of PNT

APNT R&D

https://github.com/cisagov Search "PNT"

Epsilon
Integrity Library & Toolkit

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Available Resources

https://www.cisa.gov/pnt

- Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations
- DHS S&T's GPS Whitelist Development Guide
- Epsilon Algorithm Suite: These algorithms provide end-users basic spoofing detection capabilities (e.g., detecting inconsistencies in position, velocity, and clock observables commonly provided by GPS receivers) without any modifications to the existing GPS receiver.
- Paper on Improving the Operation and Development of GPS Equipment Used by Critical Infrastructure
- PNT Integrity Library: This library provides users a method to verify the integrity of Global Navigation Satellite System (GNSS)-based PNT sources. It provides a scalable framework for GNSS-based PNT manipulation detection that offers varying levels of protection based on the available data.
- Radio Frequency Interference Best Practices Guidebook
- Report on PNT Backup and Complementary Capabilities to the GPS
- Time - The Invisible Utility: two quick reference guides designed for organization leaders (corporate level) and IT professionals and staff (technical level) on the importance of accurate and resilient timing.
- Corporate-level fact Sheet (for organization leaders)
- Technical-level fact Sheet (for IT and staff)
- Resilient PNT Conformance Framework
- Time Guidance for Network Operators, Chief Information Officers, and Chief Information Security Officers
- Understanding Vulnerabilities of Positioning, Navigation, and Timing (PNT) fact sheet