PNT Enables and Enhances Everyday Life

GPS is a free low-level RF signal for all; extreme vulnerability to jamming and spoofing

UNCLASSIFIED

Photos provided by Adobe Stock Free Collection: Photos, Vectors, Videos | Adobe Stock

PNT Executive Order 13905

- Recognizes that in many cases, GPS is the sole source of PNT.
- Loss of GPS could significantly disrupt large portions of the economy.
- Critical Infrastructure systems can maintain operation if properly designed to manage GPS disruptions.
- Requires identification of significant risk to critical infrastructure due to unmitigated PNT vulnerabilities.

PNT Executive Order 13905 Cont.

- CISA will work with industry to encourage and facilitate the adoption of the concept of “responsible use of PNT.”

- Coordinate with Sector Risk Management Agencies (SRMAs) and build a common framework for assessing and mitigating PNT-related risk.

- Requirement of PNT risk mitigation plans with future government contracts.

Understanding PNT as a National Critical Function

Providing PNT is an NCF that enables or enhances other NCFs

Helps realize the cross-cutting risks and associated dependencies

Loss of GPS has been estimated at $1 billion/day due to either the loss or degradation of the NCFs Squared-off on the right

DHS encourages the “Responsible Use of PNT” in accordance with EO 13905 to improve the security and resilience of supported NCFs

It is the responsibility of the PNT user to be able to remain secure and resilient to at least short-term disruptions

This is accomplished through the Profile developments and Federal Contract Language

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

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.

UNCLASSIFIED

National Risk Management Center

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

NRMC is the Nation's Risk Advisor!

MISSION PRIORITIES:

- Analyzes most strategic risks to our Nation's critical infrastructure
- Leads public/private partnership initiatives to manage priority areas of national risk
- Collaborates with the private sector and other stakeholders to better understand future threats.

Latest GPS Disruption Concerns

- **GPS disruption that lasted just over thirty-three (33)** hours in the vicinity of Denver Airport, which was accidentally interfering with the GPS L1 signal.
- **This incident effected critical infrastructure that relied on the GPS signal for PNT services**, which included (1) air, surface and rail traffic and (2) synchronous communications towers and (3) health care data transfer services using GPS timing signals.
  - Expecting GPS service to be reliable, some owners of systems believed the probable cause was not a loss of signal, but a system failure of some type. The area affected was in excess of 50 miles.
  - **CISA has published on their public page CISA Insights on this issue (TLP Clear) and best practices for setting up GPS User Equipment.**
  - Synchronous towers with Rubidium holdover for timing began to fail and isolate during this time
  - More robust back up systems only realized there was a loss by checking logs at CISA's request

UNCLASSIFIED

Latest GPS Disruption Concerns Cont.

- **This unintentional interference incident, initiated the established national coordination process**, which has several department and agencies operations centers responsible for monitoring and coordinating response – it still took over 33 hours, since there were persistent issues for the government to handle – the CRUCIBLE Reporting process from the Government's response was immediate.

- **Unfortunately, there was a similar, but intermittent, GPS disruption that occurred in the Dallas Fort Worth area that lasted 55 hours** during October 2022. The situation was never resolved – the incident is still under investigation.

- **Improving interference detection and mitigation (IDM) of GPS signal interference is a priority of CISA**. NRMC is working to improve the reporting and the response process down to the state, local, tribal and territorial government level.

WHAT CAN CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS DO?

Installation and Operation Strategies

- Obscure antennas
- Provide decoy antennas
- Carefully select antenna locations
- Employ blocking antennas
- Introduce redundancy
- Calibrate
- Avoid using low elevation signals
- Use position hold for stationary timing receivers
- Employ high-quality holdover devices
- Add a sensor/blocker
- Practice good cyber hygiene

Strategies for Manufacturers

- Extend data spoofing whitelists to sensors
- Plan for growth
- Implement software assurance
- Return to known good state
- Address all components
- Enable secure remote access and management
- Enhance anti-jam capabilities
- Enhance anti-measurement spoof processing
- Implement anti-data spoofing
- Use more GPS signal types
- Instrument receivers capable of capturing data

Positioning, Navigation, and Timing (PNT) Technologies

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

CRITICAL AND EMERGING TECHNOLOGIES LIST UPDATE

- Diversified PNT-enabling technologies for users and systems in airborne, space-based, terrestrial, subterranean, and underwater settings

- Interference, jamming, and spoofing detection technologies, algorithms, analytics, and networked monitoring systems

- Disruption/denial-resisting and hardening technologies

Closing Remarks – 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

Report Linked Here

Key Findings:

“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.”

Key Recommendations:

- **End Users are Responsible for Short Term Disruptions**
- **Encourage Diversity and segmentation** (multiple systems are available – encourage adoption)
- **Improve the design of Critical Systems** (DHS is participating in IEEE P1952 (PNT User equipment Standards)
- **Focus: R&D** that facilitates transition and adoption

UNCLASSIFIED

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA