IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

UNDERSTANDING VULNERABILITIES OF POSITIONING, NAVIGATION, and TIMING

Positioning, Navigation, and Timing (PNT) services are an integral part of our everyday life. From mobile phone applications to manufacturing and farming, our interconnected society is dependent on PNT services to synchronize operations over large areas and to know exactly where devices are enabling automation. In many cases, the U.S. Global Positioning System (GPS) is the sole source of PNT. Consequently, the loss of GPS could significantly disrupt large portions of our economy.

The Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center (NRMC) works with government and industry partners to strengthen the security and resiliency of the national PNT ecosystem from the risks of both intentional and unintentional threats.

EXECUTIVE ORDER 13905

Our society is becoming increasingly digitized. A key enabler of this digitization is the ability to synchronize operations over large areas and to know the exact location of devices. In many cases, GPS is the sole source of PNT, which enables synchronization and location. Consequently, the loss of GPS could significantly disrupt large portions of our economy. However, as we have seen from past GPS anomalies, critical infrastructure systems can maintain operations if they are properly designed and configured to manage GPS disruptions.

On February 12, 2020, then President Donald J. Trump issued Executive Order (E.O.) 13905, Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services.[1] The E.O. requires identification of significant risk to critical infrastructure due to unmitigated PNT vulnerabilities. In response, CISA will work with industry to encourage and facilitate the adoption of the concept of "responsible use of PNT" as defined in the E.O. Additionally, CISA will coordinate with the Sector Risk Management Agencies (SRMAs) in the development of PNT Profiles, which will provide a common framework for assessing and mitigating PNT-related risk. Future contracts with the government for services dependent on PNT will require PNT risk mitigation plans.

WHY SHOULD CRITICAL INFRASTRUCTURE OWNERS/OPERATORS BE CONCERNED?

Due to the reliability and availability of GPS, some critical infrastructure systems have been designed assuming that GPS will always be available and accurate. However, if critical infrastructure systems are designed using this assumption, they can rapidly degrade or fail if PNT data is unavailable or corrupted.

> On April 6, 2019, a $500M radio system supporting New York City government operations crashed and remained offline for days due to improperly configured GPS receivers. On that same day, dozens of international flights were cancelled due to the same configuration error.

Disrupting or corrupting PNT signals used to be the purview of nation-states. This is no longer true. With a few hundred dollars of commercially available hardware and free software, hackers can block or replace GPS signals. In addition, GPS signals may be disrupted due to system errors, user equipment failure, or environmental effects such as solar flares. Analysis by DHS indicates improperly designed critical infrastructure systems will degrade or fail if PNT services are corrupted or disrupted. The use of PNT is often hidden, which creates unrecognized risk.

[1] Executive Order 13905 Link: https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing

WHAT CAN CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS DO?

Collaborate with CISA and SRMAs to:

- Conduct vulnerability assessments of critical systems to identify and mitigate PNT-related risk
- Develop PNT Profiles to enable reliable and repeatable assessments
- Adopt the concept of "responsible use of PNT" when developing and configuring critical infrastructure systems to mitigate known issues related to PNT overdependence

EXAMPLES OF KNOWN PNT DEPENDENCIES

Critical Infrastructure Sector	Areas Dependent on PNT (Not all inclusive)				
Chemical	Earth Drilling	Pipelines	Industrial Control Systems (ICS)	All Modes of Transportation	—
Communications	Wired/Wireless	Internet of Things	Health Care Monitoring	—	—
Critical Manufacturing and Defense Industrial Base	Supervisory Control and Data Acquisition (SCADA)	ICS	Monitoring	Workforce/ Asset Tracking	—
Dams	Power Generation	SCADA	Waterway Surveillance	—	—
Energy	Measurement	Monitoring	Control Systems	Automation	Protection
Financial Services	System Forensics	Regulatory Requirements	Time Stamping	—	—
Food and Agriculture	Food Sourcing	Food Control	Workforce/ Asset Tracking	Environmental Protection	Automation
Information Technology	Smart Devices	Cloud Operations	Incident Investigations	Boot/Runtime Security	—
Transportation	Aviation	Maritime	Pipelines	Rail	Roadway
Water and Wastewater Systems	Power Generation	SCADA	Waterway Surveillance	—	—

PNT RESOURCES

- PNT webpage: cisa.gov/pnt
- GPS webpage: gps.gov
- NRMC Resources: cisa.gov/nrmc-resources