ASSURED POSITION, NAVIGATION, AND TIMING (PNT) SUMMIT

PNT RISK MANAGEMENT

MAY 2023

Michael Roskind
May 2023

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.

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 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.

Our Concern: Over-Dependence on GPS

- Widespread use, and possible dependence, on GPS across U.S. critical infrastructure
- GPS and GNSS signals extremely weak, unencrypted and difficult to authenticate
  - < 1 billionth of a watt (trying to see a 20-watt light bulb in California from New York at noon)
  - Easy to Jam (Less than $50 on the internet (illegal to buy)
  - Easy to Spoof (Replace the real GPS signal with an errant signal using parts less than $250)
- Many GPS receivers designed without security considerations to address jamming and spoofing
- Many (most) critical infrastructure systems are designed assuming that GPS data is always available and always reliable

Over 900,000,000 GPS/GNSS receivers in the U.S.

PNT Executive Order 13905

Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing (PNT) Services, February 12, 2020.

- To strengthen national resilience, the federal government must foster the responsible use of PNT services by critical infrastructure owners and operators.
- “Responsible use of PNT services” means 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” means a description of the responsible use of PNT services—aligned to standards, guidelines, and sector-specific requirements—selected for a particular system to address the potential disruption or manipulation of PNT services.
- NIST provided all stakeholders the Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services as a set of guidelines using five processes: Identify, Protect, Detect, Respond and Recover. See the full document at https://doi.org/10.6028/NIST.IR.8323
    - NRMC is conducting an SRMA-level Working Group (Government Only) on the collaboration and execution effort on sector-specific vulnerability test/assessment outreach, education and execution, which will develop PNT profiles and Federal Contract language as required by EO 13905.

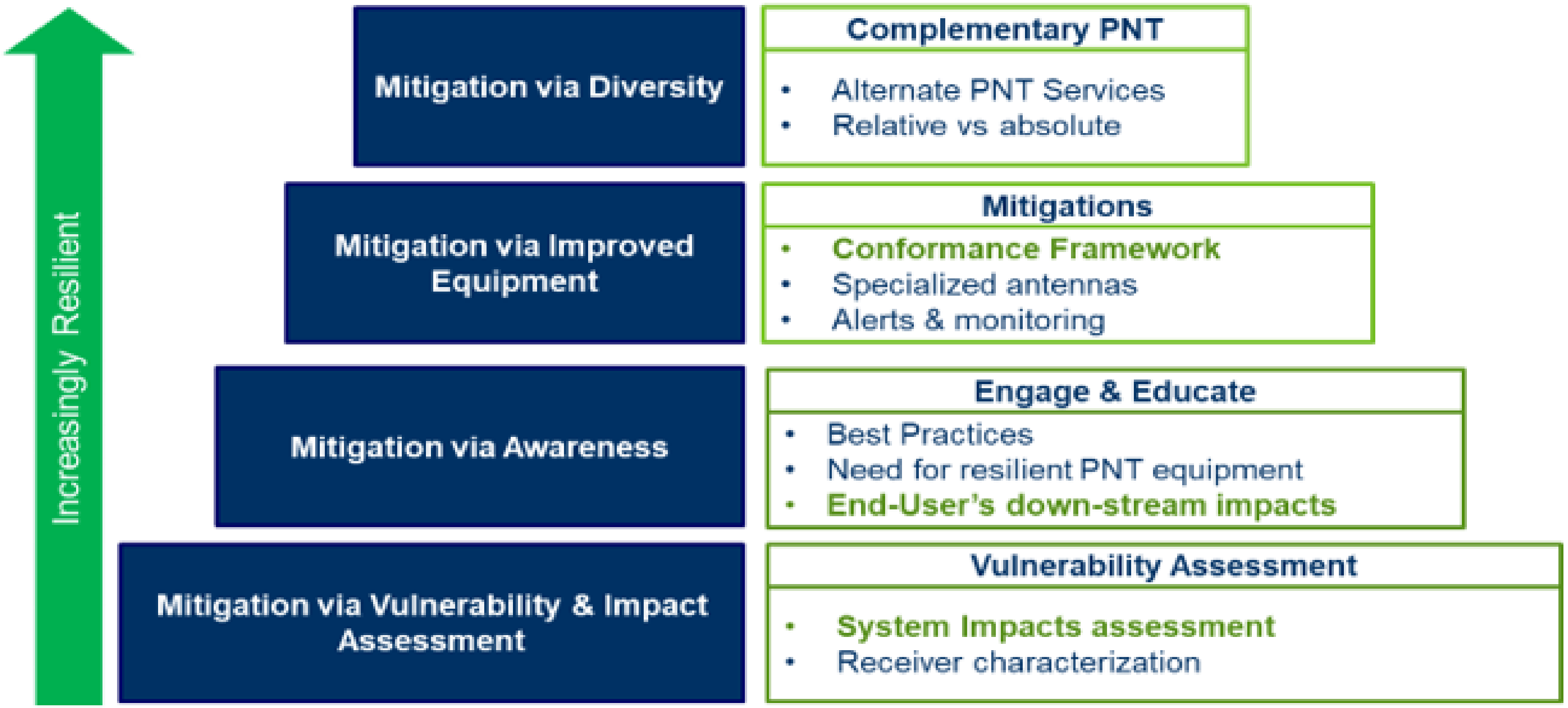
PNT Classification as a Cyber Incident

NISTIR 8323 Page 96

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. For example, PNT data is generated by cyber systems**. Protection of the devices and systems used to generate PNT data should be considered part of cybersecurity.** [NIST SP 800-53]

NRMC PNT Strategic Overview

Holistic view with a layered approach



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 than just the receiver; NRMC approaches this from a systems level view.

Federal Contract Language Overview

The Executive Order 13905, requires the Sector Risk Management Agencies upon development of their PNT Profile to "develop contractual language for inclusion of the relevant information from the PNT profiles in the requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services."

- While most PNT profiles are still under development by the SRMAs, NRMC is leading an interagency Federal Contract Language Working Group to develop base-level guidelines to improve the resiliency of PNT information systems and PNT operational technologies acquired by the federal government.
- The guidelines also provides a point of reference for U.S. critical infrastructure owners and operators regarding the reduction of risks inherent to over reliance on GPS.
- The proposed guidelines which informs PNT requirements when designing or acquiring PNT systems. It is an advisory PNT risk management resource for contract developers, contracting officers and respondents to contracts.
- The proposed guideline puts forward a workflow to assess and analyze risk in terms of PNT acquisitions and resiliency of those products, systems, or services.
- The Working Group's intent is to do no harm or cause issues for the sectors when developing their sector specific contract requirements.

CISA R&D on the Responsible Use of PNT

FY 2022 Efforts (ongoing into FY 23)

- **Participation in the IEEE P1952 Working Group**, which incorporate numerous industry stakeholders: Open to the public to participate in the UE standards.
- **Examine the Timing Requirements for 5G and LMR** using the Critical Infrastructure Research Institute (CIRI), followed by validation of critical infrastructure's ability to connect to an alternate timing solution for 5G and LMR as use cases.

FY 2023 Efforts: CISA will work with DHS S&T on their approach for the Infrastructure Investment Jobs Act (IIJA) under their program titles Critical Infrastructure Security and Resilience Research (CISRR)

- **Providing Subject Matter Expertise (FFRDC) to DHS Sectors** which are voluntarily willing to participate in Vulnerability Testing (Section 4c EO 13905). NRMC is focused on education and adoption of PNT resilience best practices.
- **NRMC-DHS S&T Investigation of alternate Timing Solutions.** Having responsibility as state emergency managers or support to state emergency managers during national level disaster declarations, State National Guard leadership is looking to mitigate the effects of catastrophic loss of GPS/GNSS services' effect on their mission essential functions, through a concept named NITRO. Designed to support state-owned timing dependent systems, this is a SWOT analysis of the physical, technical, social (governance), legal and economic considerations of the concept's adoption viability, to extend the timing technology, from state government owned infrastructure to private timing dependent critical infrastructure.

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

For more information:

www.cisa.gov

www.cisa.gov/pnt

www.gps.gov

Questions?

Email: michael.Striffolino@cisa.dhs.gov
Michael.Roskind@cisa.dhs.gov
Phone: 202-834-0286

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA