Position, Navigation and Timing for National Security

MICROCHIP

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

SMART | CONNECTED | SECURE

Barry Dropping

November 2021

Agenda

PNT vulnerabilities and the market dilemma

What are countries doing to address the threat

Protection strategies and recommendations

Critical Infrastructure Sectors Depend on PNT

1. Chemical Sector
2. Communications Sector
3. Dams Sector
4. Emergency Services
5. Financial Services
6. Government Facilities
7. Information Technology
8. Transportation
9. Commercial Facilities
10. Critical Manufacturing
11. Defense Industrial Base
12. Energy
13. Food and Agriculture
14. Healthcare and Public Health
15. Nuclear, Materials, and Waste
16. Water and Wastewater Systems

The Dilemma in the Market

Is the operator aware of PNT vulnerabilities?

PNT Vulnerability

Not aware of problem

Don’t believe there is a problem

GNSS Outages Continue to Make News

Thousands of GNSS jamming and spoofing incidents reported

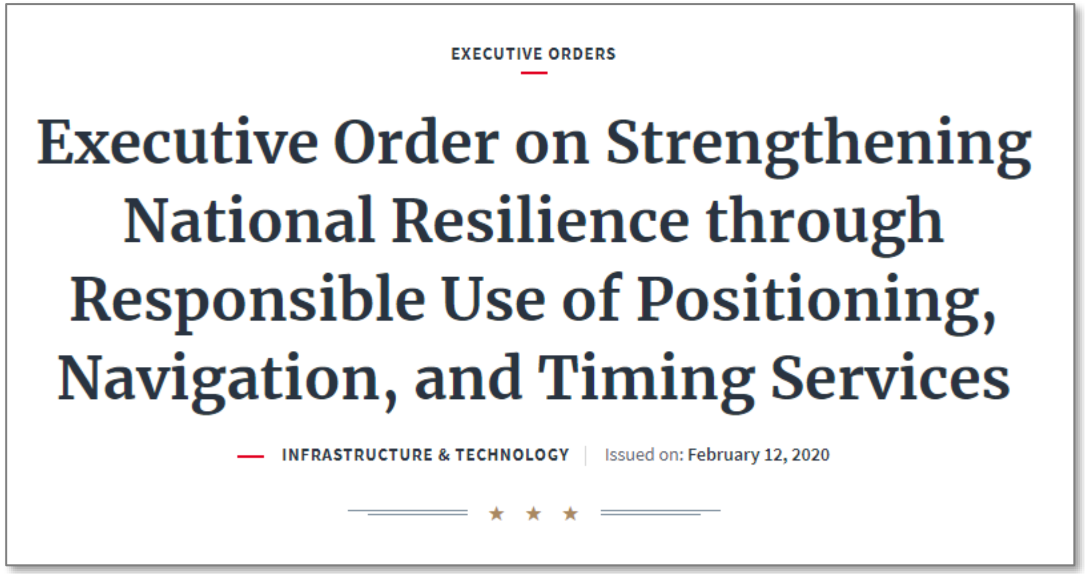
China: Intermittent GPS signal loss experienced by aircraft landing at Harbin airport in north-eastern China is traced to a jammer installed at a nearby pig farm.

Mexico passes an anti-jammer law, having discovered that GPS jammers are used in 85% of cargo vehicle thefts in the country.

Norway: GPS jamming once again causes problems in the far north of Norway, close to the Russian border.

Global: Echoing MARAD warning, Fortune reports that GPS outages are now standard occurrences on commercial flight routes between the US, Europe and the Middle East.

Executive Order on PNT Resilience



EXECUTIVE ORDERS

Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services

INFRASTRUCTURE & TECHNOLOGY | Issued on: February 12, 2020

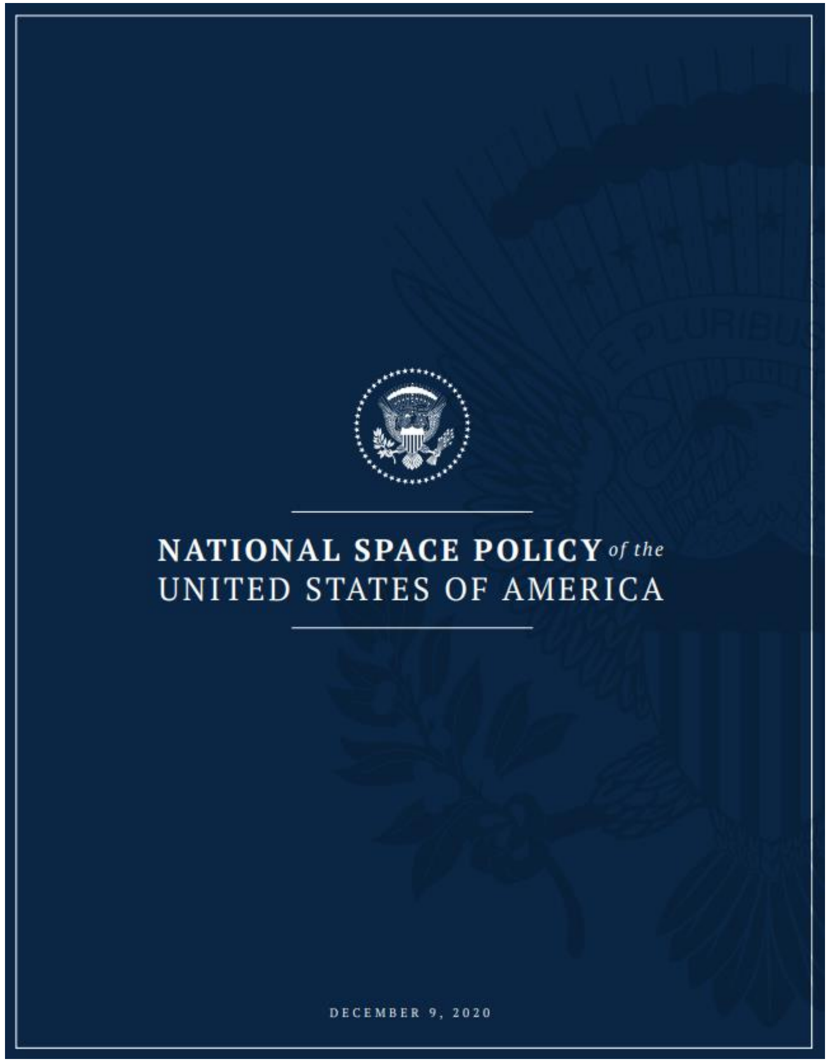
★ ★ ★

International Collaboration →

Key Initiatives
Department of Transportation (DOT) trial terrestrial eLoran as key solution
Time Guidance document by CyberSecurity Infrastructure Security Agency (CISA)
Office of Science and Technology (OSTP) issues RFI
NIST draft Cybersecurity Profile for the Responsible Use of PNT Services
DHS issued PNT Conformance Framework document

National Space Policy (December 2020)

PNT Resilience a Key Part of the Policy

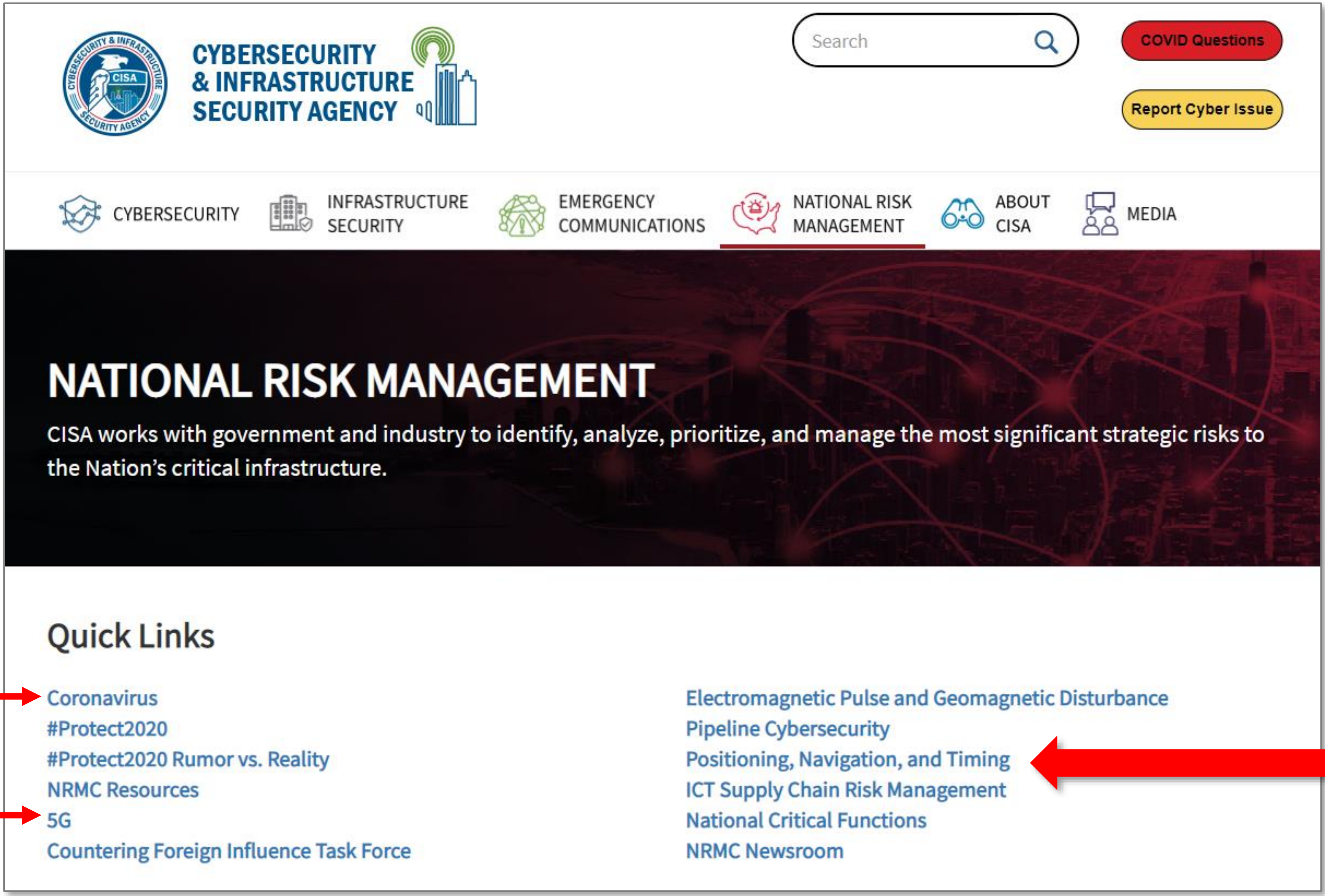


NATIONAL SPACE POLICY *of the* UNITED STATES OF AMERICA

DECEMBER 9, 2020

- Improve the cybersecurity of GPS
- Engage with international GNSS providers to encourage interoperability
- Invest in activities to detect, analyze and mitigate to increase resilience against harmful interference to GNSS
- Promote diverse complimentary PNT approaches

Cybersecurity & Infrastructure Security Agency (CISA)



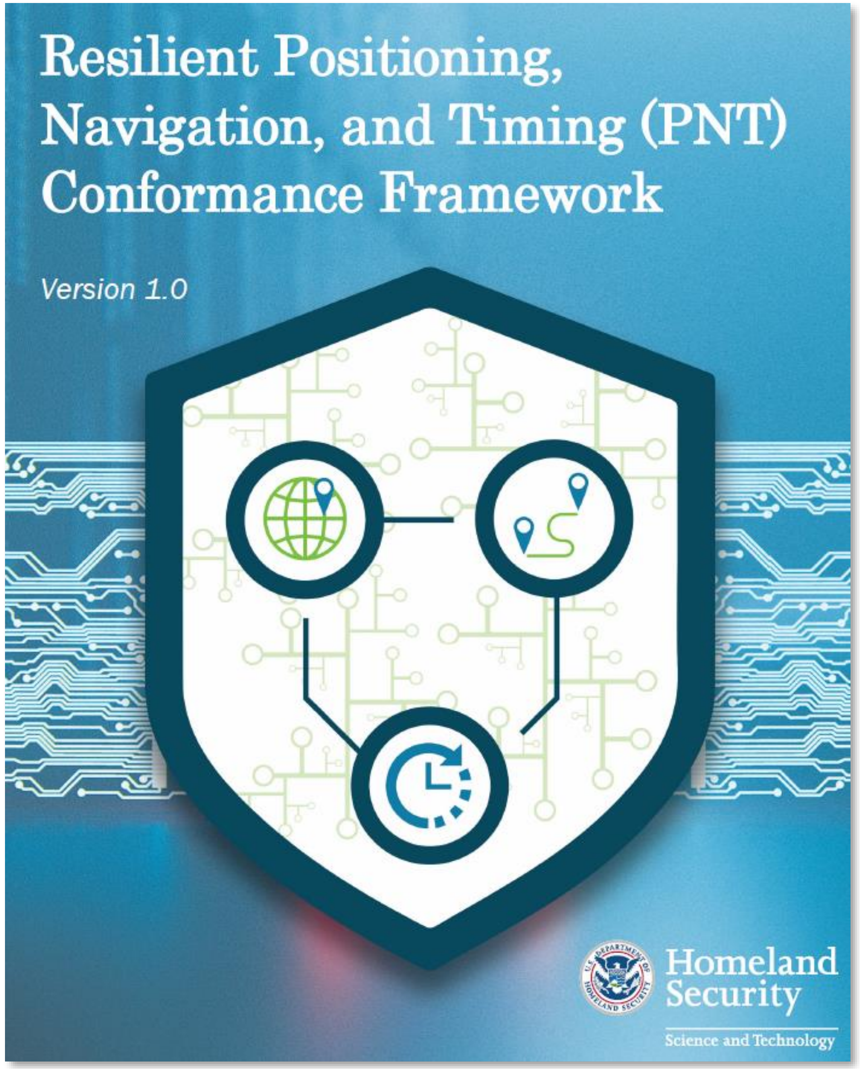
NATIONAL RISK MANAGEMENT

CISA works with government and industry to identify, analyze, prioritize, and manage the most significant strategic risks to the Nation's critical infrastructure.

Quick Links

- Coronavirus
- #Protect2020
- #Protect2020 Rumor vs. Reality
- NRMC Resources
- 5G
- Countering Foreign Influence Task Force
- Electromagnetic Pulse and Geomagnetic Disturbance
- Pipeline Cybersecurity
- Positioning, Navigation, and Timing
- ICT Supply Chain Risk Management
- National Critical Functions
- NRMC Newsroom

Resilient PNT Conformance Framework (December 18, 2020)



Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework

Version 1.0

- The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover from disruptions.

- The framework focuses on achieving resilience of PNT User Equipment and services. It is developed around the Presidential Policy Directive on Critical Infrastructure Security and Resilience.

Core Functions of Resiliency

Prevent
Respond
Recover

- **Prevent:** Ideally threats are prevented from entering a device or system, however, it must be assumed that it will not be possible to stop all threats.

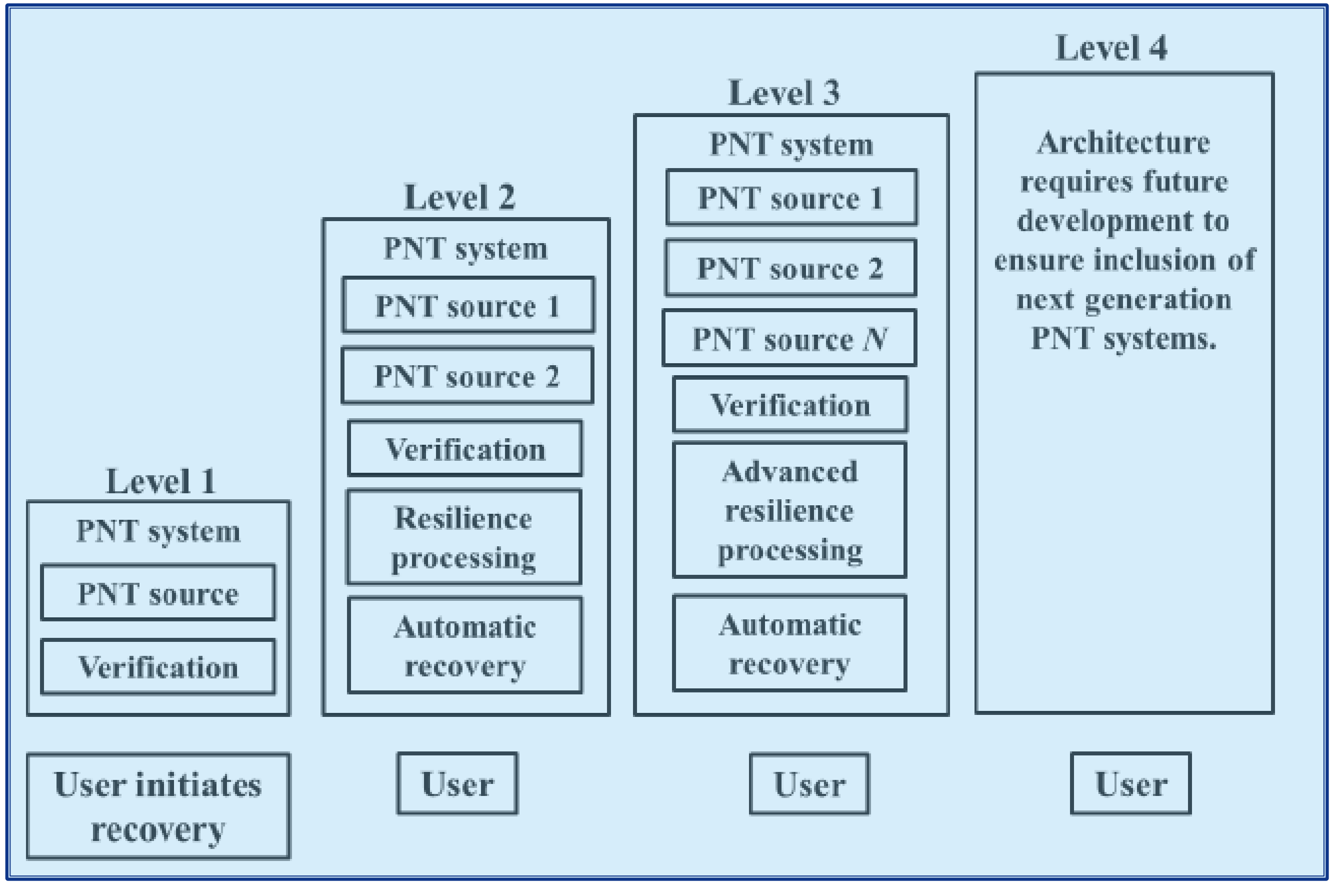
- **Respond:** detect atypical errors or anomalies and take protective actions such as mitigation, containment and reporting.

- **Recover:** from atypical errors to return to a proper working state and defined performance.

Resilience Levels

Resilience Levels build upon each other

- **Level 1:** Ability to recover
- **Level 2:** Identify compromised PNT sources but able to continue providing a PNT solution
- **Level 3:** Operate with a bounded degradation and ability to cross-verify between PNT solutions
- **Level 4:** Ability to operate with "no degradation to performance"



Level 1
PNT system
PNT source
Verification
User initiates recovery

Level 2
PNT system
PNT source 1
PNT source 2
Verification
Resilience processing
Automatic recovery
User

Level 3
PNT system
PNT source 1
PNT source 2
PNT source *N*
Verification
Advanced resilience processing
Automatic recovery
User

Level 4
Architecture requires future development to ensure inclusion of next generation PNT systems.
User

Source: Resilient PNT Conformance Framework , December 18, 2020

Visibility Enables Better Security

Visibility of threats enables pro-active security

Alarm System

Sensors - inside the house

Alarm System

Cameras - outside the house

Summary

Position, Navigation and Timing for National Security

DHS Resilient PNT

Level 4 Protection

GNSS incidents continues to grow at a dramatic rate, impacting multiple critical infrastructure sectors

The recently published “Resilient Positioning, Navigation and Timing Conformance Framework” guidelines are the result of global participation by PNT industry experts

Commercial suppliers provide a wide range of field proven PNT protection solutions for national security

Thank You