RSAConference2021

May 17 – 20 | Virtual Experience

RESILIENCE

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

America (and the World) Has a GPS Problem

Executive Order 13905 on PNT

Issued February 12, 2020

- Promote responsible use of PNT services
- Minimize impact to nation if disruption or manipulation occurs
- Focus on critical infrastructure
- In practice, applicable to all systems using PNT services

Why PNT? Why Now?

Surveying & Mapping

Air Traffic Control

Personal Navigation

Power Grids

Precision Agriculture

Telecommunications

Transit Operations

Supply Chains

Financial Markets

Oil Exploration

Shipping & Maritime

Emergency Services

Space Systems

Healthcare

Global Navigation Satellite Systems (GNSS) Lack Integrity Checks

Common issues

- All GNSS systems broadcast a weak signal and an unencrypted data stream
- All systems can be jammed (denial of service) with a $30 jammer
- All system signals can be manipulated (person in the middle attack)
  - $200 software defined radio
  - Software from GitHub
- Other geolocation and timing services are available

Cautionary Tale: Black Sea Spoofing Event

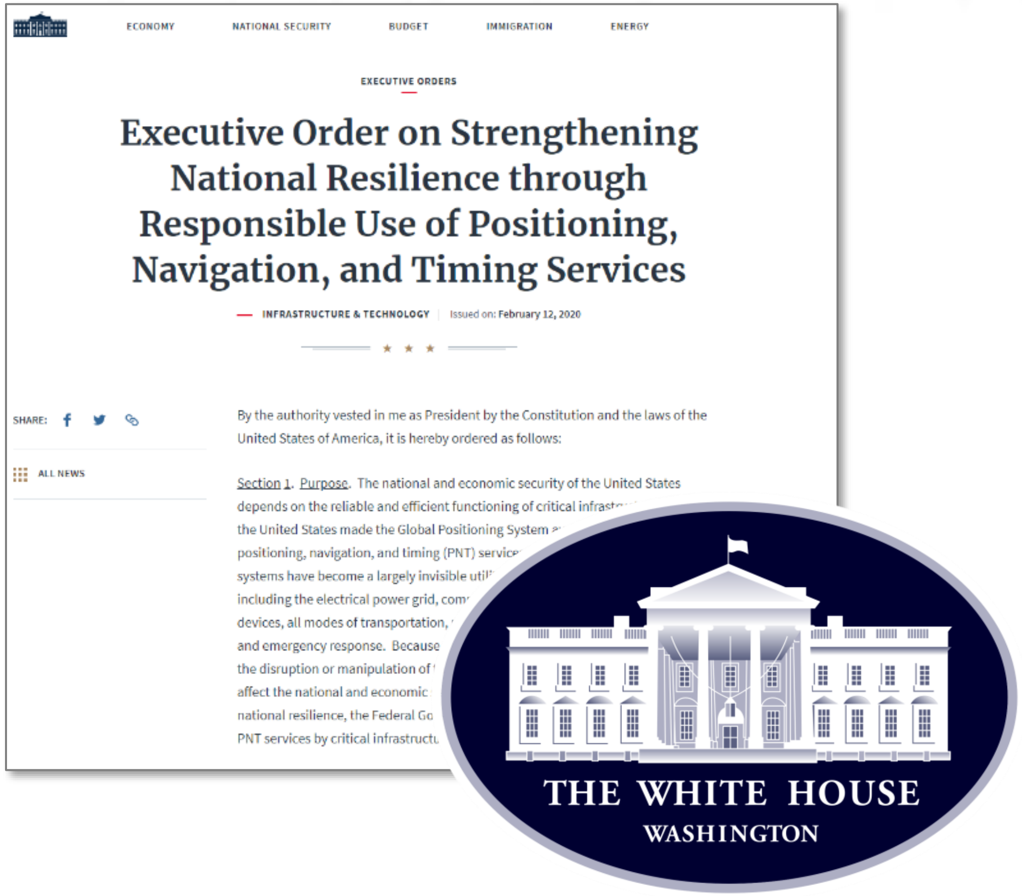
Cautionary Tale: GPS Week Number Rollover

Cautionary Tale: C&O Canal

Image courtesy DC Fire and EMS

Responsible Use of PNT Services is Essential

Responsible use of PNT is defined as deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services **minimally affects critical infrastructure operations**.



EXECUTIVE ORDERS

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

INFRASTRUCTURE & TECHNOLOGY | Issued on: February 12, 2020

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

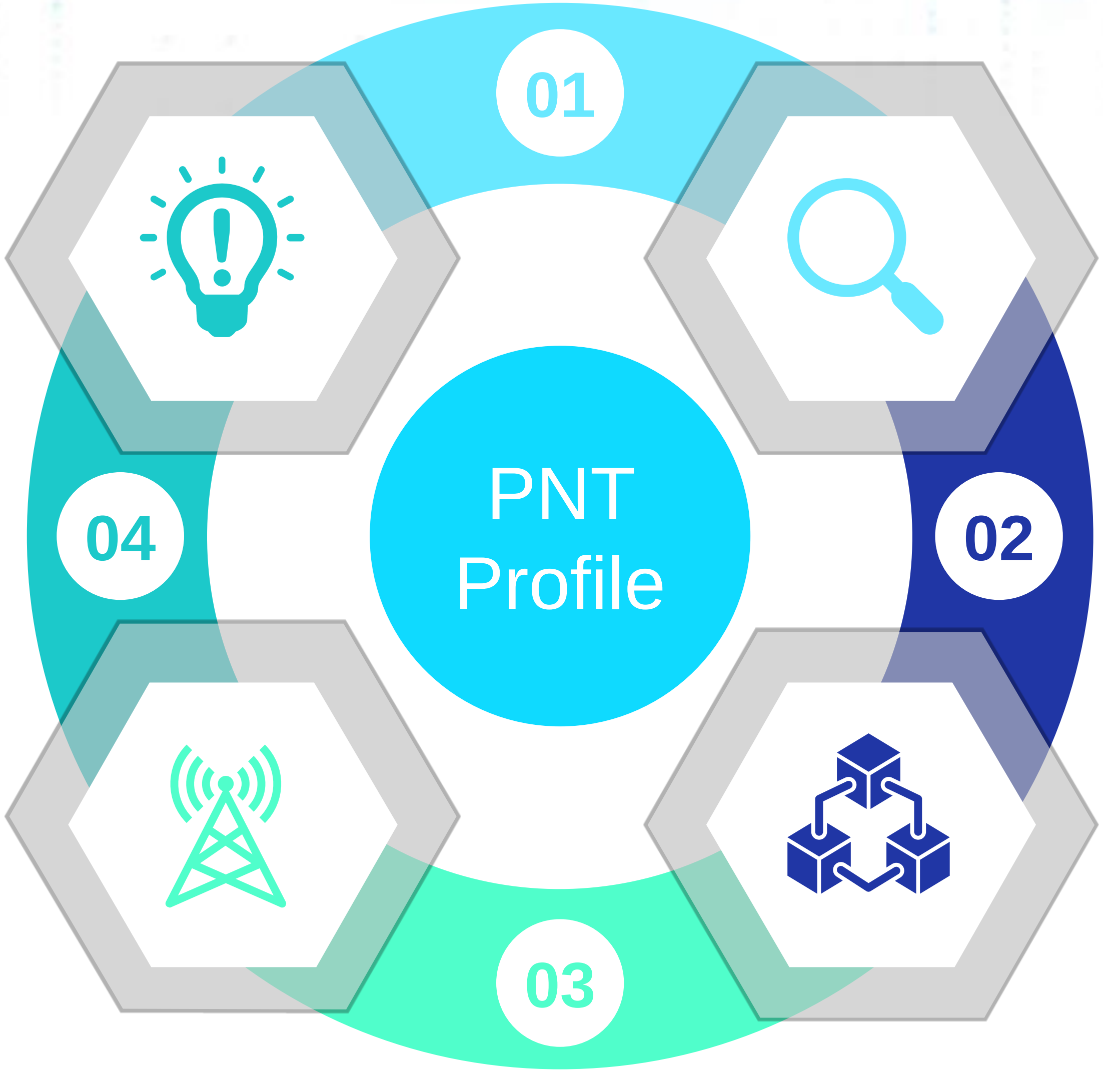
Section 1. Purpose. The national and economic security of the United States depends on the reliable and efficient functioning of critical infrast
the United States made the Global Positioning System
positioning, navigation, and timing (PNT) service
systems have become a largely invisible util
including the electrical power grid, com
devices, all modes of transportation,
and emergency response. Because
the disruption or manipulation of
affect the national and economic
national resilience, the Federal Go
PNT services by critical infrastructu

RSAConference2021

NISTIR 8323

Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing Services

PNT Profile: Purpose



Manage the risk to these systems

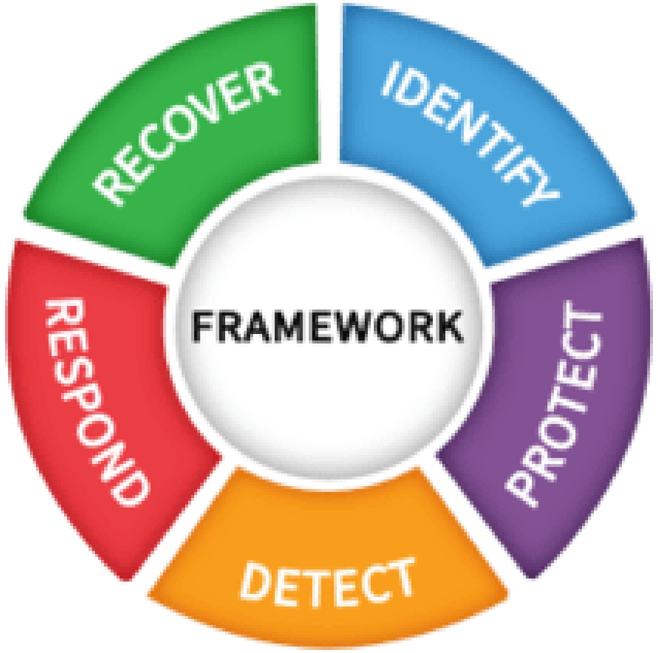
Identify systems dependent on PNT

Identify appropriate PNT sources

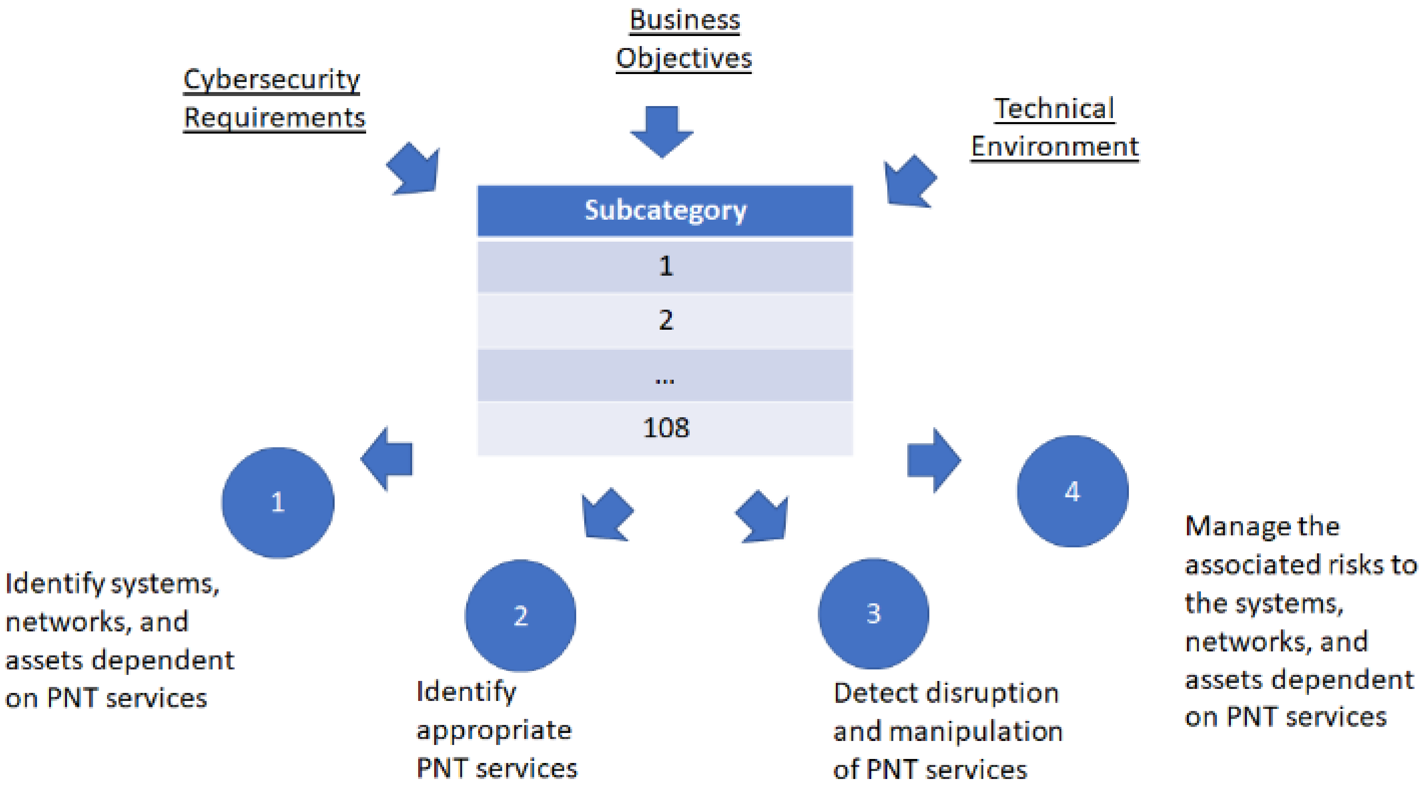
Detect disturbances and manipulation of PNT services

PNT Profile Development Process

- Open, transparent, and collaborative
- Engage with primary stakeholders
- Focus on critical infrastructure
- Leverage the NIST Cybersecurity Framework



Cybersecurity Framework Profiles



Subcategory
1
2
…
108

1. Identify systems, networks, and assets dependent on PNT services

2. Identify appropriate PNT services

3. Detect disruption and manipulation of PNT services

4. Manage the associated risks to the systems, networks, and assets dependent on PNT services

Use the PNT Profile along with your unique cybersecurity requirements, business objectives, and technical environment to meet the objectives of the Executive Order

Content of the PNT Profile

Guidance on how to apply the subcategory to organizations that rely on PNT services

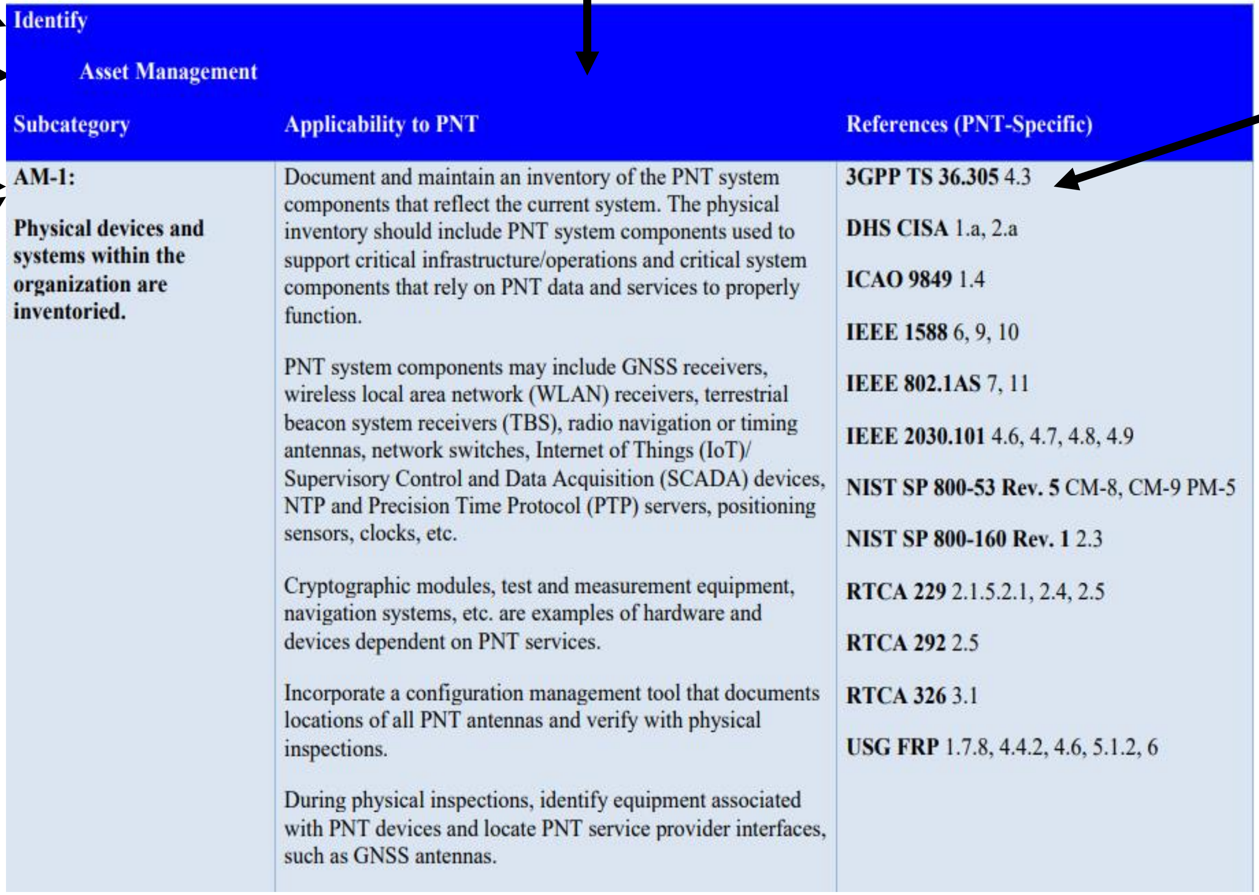
Function

Category

Subcategory

Subcategory ID

CSF language



Identify		
Asset Management		
Subcategory	**Applicability to PNT**	**References (PNT-Specific)**
AM-1: **Physical devices and systems within the organization are inventoried.**	Document and maintain an inventory of the PNT system components that reflect the current system. The physical inventory should include PNT system components used to support critical infrastructure/operations and critical system components that rely on PNT data and services to properly function. PNT system components may include GNSS receivers, wireless local area network (WLAN) receivers, terrestrial beacon system receivers (TBS), radio navigation or timing antennas, network switches, Internet of Things (IoT)/ Supervisory Control and Data Acquisition (SCADA) devices, NTP and Precision Time Protocol (PTP) servers, positioning sensors, clocks, etc. Cryptographic modules, test and measurement equipment, navigation systems, etc. are examples of hardware and devices dependent on PNT services. Incorporate a configuration management tool that documents locations of all PNT antennas and verify with physical inspections. During physical inspections, identify equipment associated with PNT devices and locate PNT service provider interfaces, such as GNSS antennas.	**3GPP TS 36.305** 4.3 **DHS CISA** 1.a, 2.a **ICAO 9849** 1.4 **IEEE 1588** 6, 9, 10 **IEEE 802.1AS** 7, 11 **IEEE 2030.101** 4.6, 4.7, 4.8, 4.9 **NIST SP 800-53 Rev. 5** CM-8, CM-9 PM-5 **NIST SP 800-160 Rev. 1** 2.3 **RTCA 229** 2.1.5.2.1, 2.4, 2.5 **RTCA 292** 2.5 **RTCA 326** 3.1 **USG FRP** 1.7.8, 4.4.2, 4.6, 5.1.2, 6

PNT specific references on how to implement controls to achieve the desired outcomes of the EO

Apply What You Have Learned Today

- Next week you should:
  - Read the NIST Foundational Profile for PNT Services
- In the first three months following this presentation consider:
  - Inventorying all systems and devices dependent on PNT data
  - Identifying sources and infrastructure that provide PNT information
  - Incorporating alternative PNT or time sources into your business architecture and the ability to failover to these systems during a disruption (see NIST's Time over Fiber resource)
- Within six months consider:
  - Identifying the vulnerabilities, threats, and impact should the threat be realized to assess your risk
  - Implementing procedures to detect PNT manipulation or disruption
  - Developing policies and procedures to respond to a disruption of PNT services

Summary

- The use of PNT data or services in your organization may not be obvious
- Organizations must understand the risks posed by dependencies on PNT services and define a risk management plan
- The NIST PNT Profile can help organizations prioritize PNT-related cybersecurity measures

National Institute of Standards and Technology
U.S. Department of Commerce

https://www.nist.gov/pnt

https://www.cisa.gov/pnt