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

NIST IR 8323

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

Jim McCarthy / NIST
Ya-Shian Li-Baboud / NIST
Orolia
March 24, 2021

Background

Executive Order 13905 of February 12, 2020

Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services.

- Responsible use of PNT services – deliberate, risk informed use of PNT services
- If disruption or manipulation occurs, minimal impact to national security, economy, public health, and critical functions of Federal Government
- Critical infrastructure – systems/assets so vital to the US that incapacity or destruction could result in debilitating impact

Background

EO 13905

- NIST (Dept. of Commerce) responsible for delivering;
  - Sec 4. Implementation - (a): PNT Profiles within one year of EO release
  - Sec 4. Implementation - (g): GNSS-independent source of Coordinated Universal Time within 180 days of EO release

- NIST Profile (NISTIR 8323);
  - Single, foundational Profile
  - Based on NIST Cybersecurity Framework (CSF)

Overview

PNT Profile Development Process

- Open, transparent, and collaborative
- Engage with primary stakeholders, both public and private, to inform development of the PNT profile
- Focus on Critical Infrastructure - owner/operators of the electrical power grid, communication infrastructure, businesses in the transportation, agriculture, weather, and emergency response sectors, among others
- Leverage the Cybersecurity Framework to develop and issue a foundational PNT profile

Overview

PNT Profile Development Timeline

February 12,2020
PNT Resiliency Executive Order Published

May 2020
NIST Request for Information issued; hosted initial PNT profile webinar

August / September 2020
Draft annotated outline published; profile development workshop convened

October 22, 2020
Draft PNT profile published; open for public comment

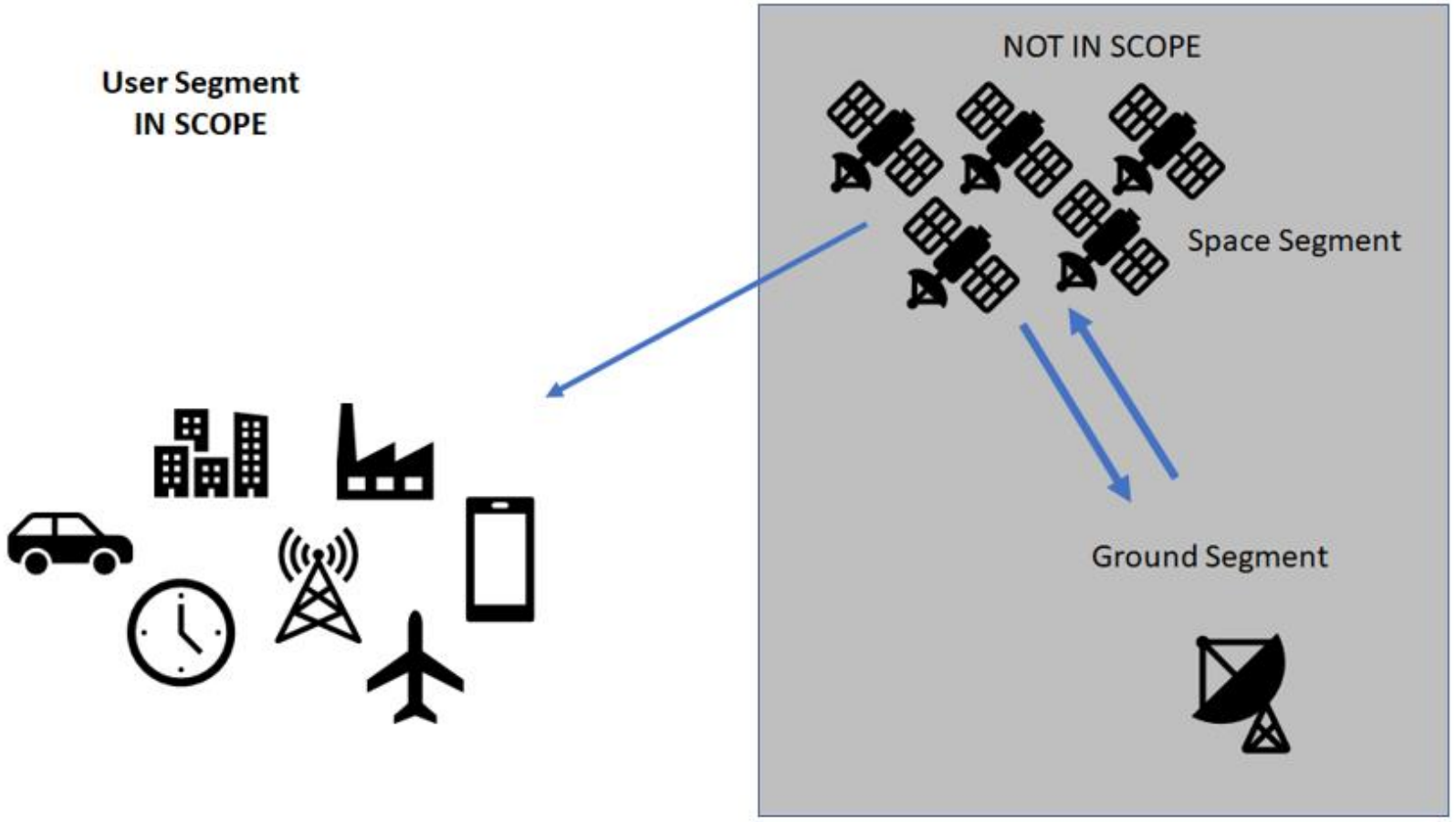
February 11, 2021
NISTIR 8323
Final PNT profile

Purpose

- Provide informed guidance to increase the responsible use of PNT services
- Apply the CSF in the context of PNT Data Use/Resilience
- Help organizations develop sector-specific PNT profiles
- Prioritize PNT-related cybersecurity measures in accordance with business or mission objectives

Overview

NIST Profile Scope



NIST Cybersecurity Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors, and uses
- Risk-based
- Meant to be paired
- Living document
- Guided by many perspectives – private sector, academia, public sector

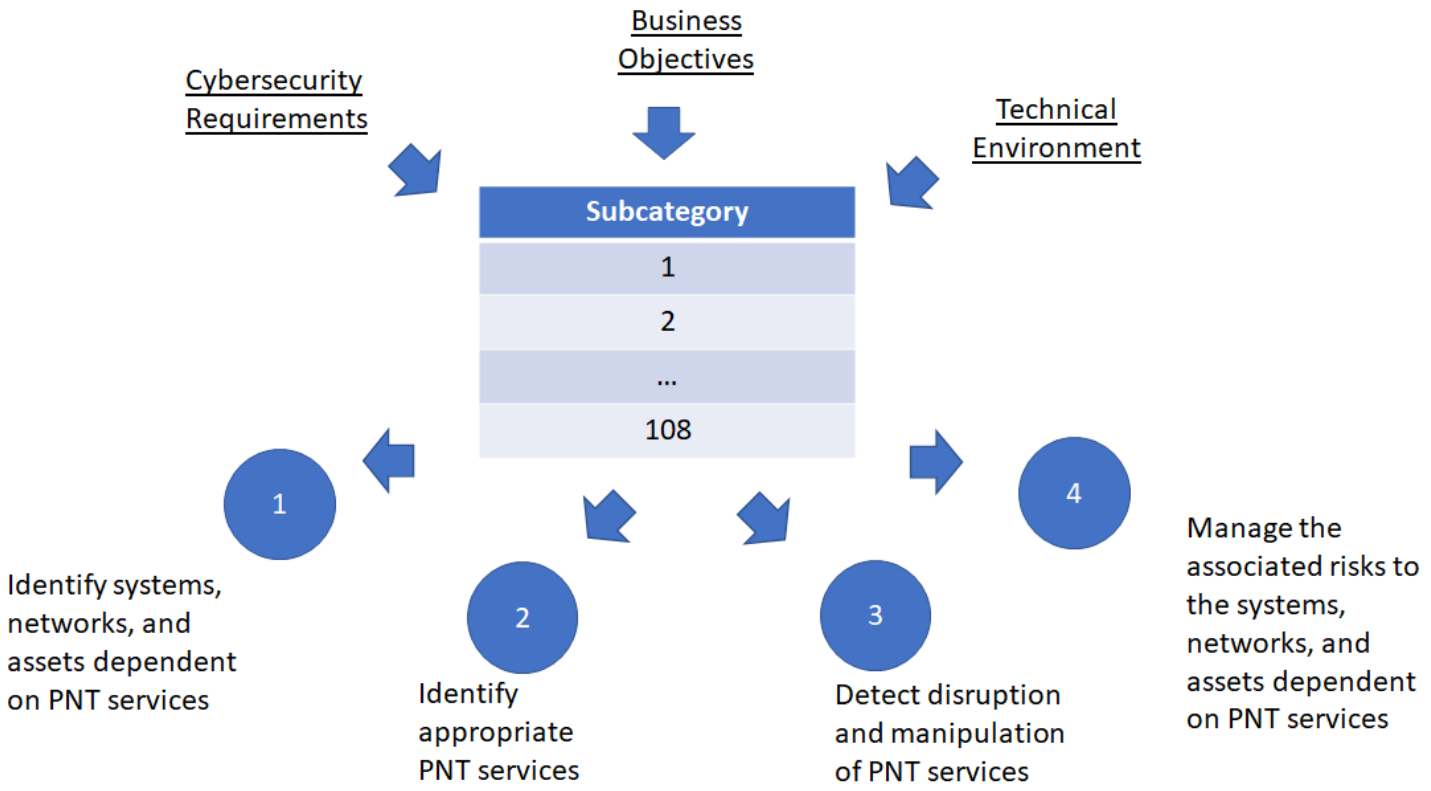
Framework Core

Establishes a Common Language

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Cybersecurity Framework Profiles



The PNT Profile along with their unique cybersecurity requirements, business Objectives and Technical Environment can be used by organizations to achieve the outcomes specified in the EO

Content of the PNT Profile

Function

Category

Subcategory

Subcategory ID

CSF language

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

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

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

Outcomes and Moving Forward

- NISTIR 8323 (Foundational PNT Profile) delivered: 02/11/2021
- Profile review: 2-year cycle, update as needed per EO 13905
- Numerous inquiries regarding ; industry / sector /sub-sector profile development
- Cybersecurity profiles with elements of PNT ???
- May 19, 2021 – Jim Platt (CISA) / Jim McCarthy (NIST) RSA Presentation on PNT Resilience

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

NIST Resources

PNT Profile :

Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services (nist.gov)

GNSS Independent Time Source:

https://shop.nist.gov/ccrz__ProductDetails?sku=78110S&cclcl=en_US

Contact NIST:

pnt-eo@list.nist.gov