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

DRAFT Annotated Outline

August 31, 2020

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

NOTES TO REVIEWERS:

NIST's objective is to deliver a PNT Cybersecurity Profile (hereafter, the Profile) that can be adapted to the needs of PNT service users in the public and private sectors. Furthermore, through the Profile, NIST seeks to increase organizational awareness of the extent to which they use and rely on PNT services.

Through the Profile development process, NIST will engage the public and private sectors on multiple occasions to include a request for information, participation in workshops, solicitation of feedback on this annotated outline, and public review and comment on the draft Profile. The Profile development process is iterative and, in the end state, will identify and promote the responsible use of PNT services from a cybersecurity point of view. This Annotated Outline is designed to engage public and private sector stakeholders on preliminary NIST thinking before publishing a draft "*Cybersecurity Profile for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services"* for public comment in October 2020.

NIST seeks insight and feedback on this Annotated Outline to improve the PNT cybersecurity profile, which is scheduled for publication in February 2021. Areas needing more input include feedback on the description of systems that use PNT services and the set of standards, guidelines, and practices addressing systems that use PNT services. NIST welcomes suggestions in these areas in addition to comments on the content within this Annotated Outline.

Editor's Note: *Italicized text within a lift out box discusses the content to include within that section. In addition, some sections include preliminary, non-italicized text to provide the stakeholder reviewers sample text of what the actual profile may contain.*

Executive Summary

Editor's Note: *This section contains a concise summary of the Profile.*

37 **Table of Contents**

38 ***Editor's Note:*** *NIST suggests the Profile have these major headings in its Table of Contents:*

39

60

61

62

1 PNT Cybersecurity Profile – Introduction

Editor's Note: *This section will summarize the purpose, objectives, and scope of the Profile for organizations that use PNT services.*

Executive Order 13905 (EO 13905), "*Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services*," was issued on February 12, 2020 [EO 13905]. It seeks to help organizations protect themselves from the disruption or manipulation of PNT services, particularly those organizations whose PNT services are vital to the functioning of U.S. critical infrastructure[1] and related technology-based industries. The Executive Order (EO) directs the Department of Commerce to develop a PNT Profile for users of PNT services.

The PNT cybersecurity profile (hereafter, the Profile) is intended for a general audience and is broadly applicable. The Profile applies to:

- Organizations that have already adopted the NIST Cybersecurity Framework (CSF)[2] to help identify, assess, and manage cybersecurity risks [NIST CSF];
- Organizations that are familiar with the CSF and want to improve their cybersecurity postures; and
- Organizations that are unfamiliar with the CSF but need to implement cybersecurity risk management frameworks for the responsible use of their PNT services.

1.1 Purpose and Objectives

Editor's Note: *This section will provide a concise purpose statement and a subset of the activities required to achieve the purpose.*

The purpose of the Profile, when used as part of a risk management program, is to help organizations manage cybersecurity risks to systems, networks, and assets that use PNT services. The Profile provides guidance for establishing risk management approaches for desired outcomes as driven by an organization's business and operational needs. The Profile is not intended to serve as a solution or compliance checklist that would guarantee the responsible use of PNT services.

[1] Critical infrastructure, as defined in the Executive order, means "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or on any combination of those matters" [EO 13905].

[2] Efforts under the PNT EO build on a previous EO, issued on February 12, 2013, that called for the strengthening of national critical and economic infrastructure against cybersecurity threats. In that EO, the President directed NIST to lead the coordination of a Cybersecurity Framework (CSF) that would reduce cybersecurity risks to critical infrastructures that rely on private sector input and existing standards, guidelines, and practices [EO 13636].

Use of the PNT Profile will help organizations to:

- Identify systems that use PNT services;
- Identify sources of PNT data;
- Protect PNT services by adhering to basic principles of responsible use;
- Detect cybersecurity-related disturbances and/or manipulation of PNT services and data;
- Address cybersecurity risk in their management and use of PNT services and data;
- Identify common threats to PNT services, [user] equipment, and data; and
- Respond to PNT service or data anomalies in a timely, effective, and resilient manner.

1.2 Scope

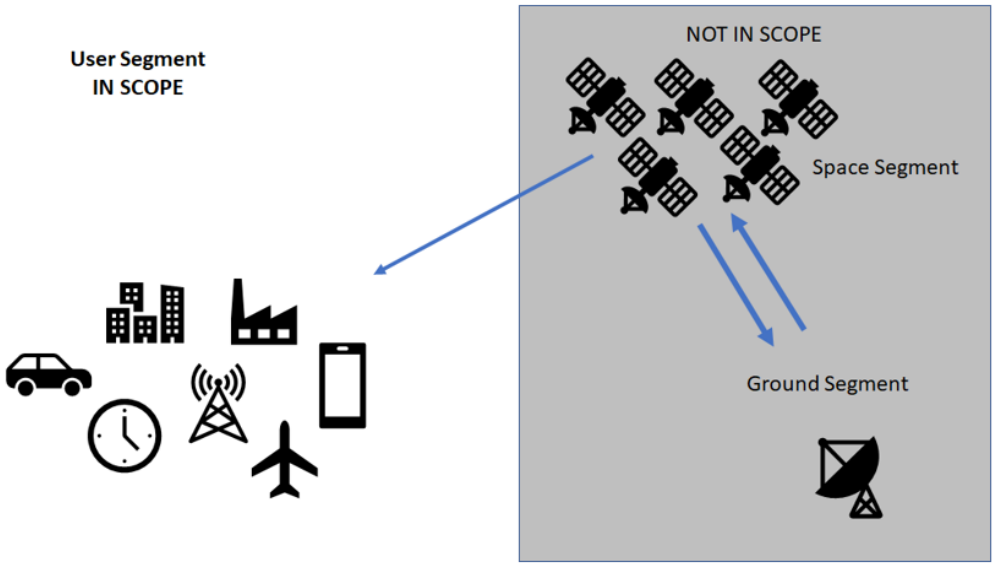
Editor's Note: *This section will highlight that the scope is for recipients of PNT services, not the service providers.*

The Profile's scope includes systems that use PNT services, including those systems that consume and then rebroadcast PNT data for consumption by other organizational entities where a PNT Service is defined as "any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof" [EO 13905]. The Profile's scope does not include source PNT signal generators and providers (e.g., a GNSS control segment or space segment as shown in Figure 1). PNT Service providers outside of an organization's control or boundary are not in the scope of this effort.

PNT Services interface with user equipment (UE) to produce PNT data, which can take the form of position, velocity, or timing information. The responsible use of PNT data requires the stakeholder to identify the dependencies of PNT data (within their components, sub-systems, and systems), evaluate the impact should the loss of PNT data be realized, and manage the residual risk.

This Profile defines the responsible use of PNT services as it relates to cybersecurity. In this case, responsible use by organizations includes the incorporation of:

- Cybersecurity risk-informed management of PNT services,
- Cybersecurity risk-based approaches that minimize the potential effects of cybersecurity disruption or manipulation of PNT services and data, and
- Deliberate planning and action regarding the secure management of PNT services.



116
117 ***Figure 1. The Scope for the PNT Cybersecurity Profile is limited to the user segment only. The provider (in***
118 ***this example, the GPS space and ground segments) is not part of this Profile.***

119 ### 1.3 Audience

Editor's Note: *This section will identify parties that will benefit from the Profile.*
120

121 This document should be used by those involved in overseeing, developing, implementing, and
122 managing the cybersecurity of systems using PNT services. This document's intended audience
123 includes:

124 • Public and private organizations that use PNT services;
125 • Managers responsible for the use of PNT services;
126 • Risk managers, cybersecurity professionals, and others with a role in cybersecurity risk
127 management for systems that use PNT services;
128 • Procurement officials responsible for the acquisition of PNT services;
129 • Mission and business process owners responsible for achieving operational outcomes
130 dependent on PNT services; and
131 • Researchers and analysts who study the unique cybersecurity needs of PNT services.

132 ## 2 How to Use the PNT Cybersecurity Profile

Editor's Note: *This section provides guidance on what can be accomplished via the profile.*
133

The Profile will help organizations develop cybersecurity PNT profiles that are appropriate for their respective sectors. The Profile will help organizations determine cybersecurity risks based on their assessments of the potential impacts of manipulation or the disruption of PNT services to business and operational objectives. The Profile is intended to help users of PNT services prioritize necessary cybersecurity activities based on business objectives. The Profile may be a tool to help organizations identify areas where standards, practices, and other guidance could help manage the risk of cybersecurity threats to systems that use PNT services.

This Profile is intended to assist an organization's risk management effort. The Profile does not prescribe regulations or mandatory practices, nor does it carry any statutory authority.

The development of a Profile by an organization is a multi-step process, including a risk assessment in which organizations consider the following:

- What processes and assets require PNT data (direct recipient of PNT services)?
- What processes and assets are dependent recipients of PNT data (i.e., identify secondary effects)?
- What is the impact to the organization should a process or asset be lost or degraded?
- What processes and assets are vulnerable?
- What safeguards are available?
- What techniques can be used to identify threats of concern?
- What techniques can be used to respond to threats of concern?
- What techniques can be used to recover pre-event capabilities?

3 PNT Cybersecurity Profile – Overview

Editor's Note: *This section contains an overview of envisioned Profile content, a short description of the kinds of PNT data users that are covered by the Profile, and an overview of PNT services. The Profile provides information on risk management, capabilities, and mapping to the NIST Cybersecurity Framework to assist with specific implementation of PNT cybersecurity. The Profile will include informative references (including existing standards, guidelines, and practices) and a glossary of terms.*

3.1 Risk Management Overview

Editor's Note: *This section reviews the risk management process.*

Risk management is the ongoing process of identifying, assessing, and responding to risk as related to an organization's mission objectives. To manage risk, organizations should understand the likelihood that an event will occur as well as its potential impacts. With this information, organizations can determine the acceptable level of risk to the PNT data and services they use to achieve their mission objectives.

As an organization analyzes its mission objectives as they relate to reliance on or use of PNT data, there are a series of guiding questions that inform the process. They include:

- What are the threats to achieving mission objectives?
- What damages can result when those mission objectives are disrupted?
- What are the most important assets for a given mission objective?
- Where does physical infrastructure affect cybersecurity infrastructure and vice versa?

An organization should also be aware of statutory and policy requirements that may have a security or safety dimension. These can be affected by cybersecurity risk or create risks downstream.

The PNT Profile supports and is informed by cybersecurity risk management processes. Using the Profile, organizations can make more informed decisions to select and prioritize cybersecurity activities and expenditures that help identify systems dependent on PNT, identify appropriate PNT sources, detect disturbances and manipulation of PNT services, manage the risk to these systems, and ensure resiliency through diversity. For critical infrastructures, PNT sources and distribution networks should be architected with multiple, independent sources; communication paths; and communication mediums. The Profile provides a starting point from which organizations can customize—based on business need and risk assessment—to develop the most appropriate processes to manage cybersecurity risk to their PNT services and data essential for the correct behavior of critical infrastructure applications.

Organizations can use the PNT Profile in conjunction with existing cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO) 31000:2018, ISO/International Electrotechnical Commission (IEC) 27005:2018, and NIST Special Publication 800-39. A full list of helpful resources will be listed in an Annex of the Cybersecurity PNT Profile.

3.2 Capabilities Overview

Editor's Note: *The section describes some of the capabilities and controls that impact the organization's ability to manage residual risk (in the context of PNT degradation or outage).*

3.2.1 Policies and Procedures

Editor's Note: *This section will discuss policies and procedures that organizations should consider when managing cybersecurity risks to systems, networks, and assets that use PNT services.*

Historically, the perceived risk to PNT services has been low while the reliance on PNT services has increased. Responsible use of PNT should include policies and procedures that map to threats to PNT services and the impacts should the threats be realized. Threat modeling may need to consider alternative PNT services (other than GNSS.) The impact to the organization may include secondary effects, such as a severe PNT data disruption that impacts a sector that provides services required by other enterprises.

Cybersecurity policies and procedures will vary in accordance with each organization's tolerance of a PNT data loss and their required PNT data precision. Though it does not add value to burden an organization with excessive requirements, there should be a level of consistency within a sector to enable collaborative efforts, such as the sharing of PNT interference events. Consistency also facilitates the acceptance or rejection of inherited risk and compatible tools; techniques and processes enable coordinated responses.

Multiple professional organizations and sector-specific stakeholders have defined PNT data security requirements and practices (references available in Appendix C) to inform PNT cybersecurity policies and procedures. In some cases, accepting degraded PNT service within a bounded uncertainty can be tolerated. Other organizations may choose to secure PNT data, provide alternative PNT services as a backup, or provide integrated PNT data from truly independent PNT service providers.

PNT policies and procedures should be reflected in an organization's continuity of operations plan (COOP). If the COOP identifies the use of legacy (or alternative) PNT, then the legacy procedures need to be exercised and updated in accordance with normal COOP procedures.

3.2.2 Security Technical Capabilities Overview

Editor's Note: *This section will discuss the capabilities of PNT services upon which an organization's systems rely, a discussion of potential threats that impact those systems, and a list of security controls that could potentially mitigate the risks.*

Responsible use of PNT services requires organizational planning that includes an adequate understanding of the technical capabilities needed to ensure appropriate levels of PNT data precision, availability, and integrity.

When considering the technical capabilities as they pertain to PNT resilience, users must consider certain technical challenges that a PNT service may encounter. PNT data may need to transfer time and frequency over long distances (for a global enterprise) while retaining accuracy (within a bounded uncertainty, 100 ns range for some applications) to Coordinated Universal Time (UTC) and availability. Should alternative PNT service providers be deemed necessary, the compatibility of implementation must be considered when investigating alternative PNT service providers. For example, while GPS notifies receivers of impending leap seconds via an announcement six weeks in advance, other PNT services only have a 12-hour advance notice. Other implementations adjust for leap seconds by introducing a frequency adjustment over an extended time interval in order to ensure that the clock continues monotonically increasing through a leap second event. However, such a frequency adjustment introduces both a time and frequency error relative to the legal UTC time [https://www.nist.gov/pml/time-and-frequency-division/services/internet-time-service-its]. GPS signals travel by line of sight, and receivers typically require at least four satellites to be in view to provide accurate position, velocity, and time (PVT) solutions. Urban canyons, mountains, trees, and atmospheric variabilities can contribute to errors in PVT solutions.

It is beneficial to consider that the analysis of potential integration of multiple and independent technologies can facilitate the detection of anomalies, provide additional precision of PNT data, and ultimately contribute to a more resilient system in the event of a disruption.

3.3 The PNT Cybersecurity Profile

Editor's Note: *This section will contain the PNT Cybersecurity Profile, which maps the functions, categories, and sub-categories of the CSF with informative references. This section contains information on how users of the profile can mitigate risks that they have deemed necessary to address based on their assessment of the PNT services they are using. This is not an exhaustive list, and the actual selection of controls (if any) must be based on a cost-benefit analysis that is consistent with the risk. NIST welcomes input on available standards, guidelines, and practices that can be considered for inclusion as informative references in the Profile.*

3.3.1 Protection of PNT Services

Editor's Note: *This section contains examples of various means to protect PNT services. This is not an exhaustive list and will not necessarily provide the appropriate level of assurance for a particular cyber ecosystem. The actual selection of mitigation techniques and controls (if any) must be based on a cost-benefit analysis that is consistent with the risk. The following sections identify, at a high level, the elements to consider in order to ensure the responsible use of PNT services. The PNT profile will incorporate these elements into actionable guidance (risk and threat mitigation techniques and controls) that organizations can implement to protect the PNT components under their purview.*

The following list contains cybersecurity considerations that are applicable to GPS-based devices, signals, data, hardware and software:

- Encrypted GPS signals for civilian use and GPS firewall technology should be considered.
- Assured mechanisms (e.g., signed, verified code) for GPS software and firmware upgrades on trusted platforms need to be in place to ensure the integrity of PNT data processing.
- Modeling and simulation—including simulated disruptions, variations in leap second implementations, and other implementation details—should be performed to exercise, test, and update these technical protections. If at all practical, open test plans and inter-sector collaboration should be encouraged so that sectors are aware of and accommodate potential cross-sector impacts.
- GPS signals may be hardened using directional antennas in conjunction with accurate tracking of individual satellites or shielded antennas that block terrestrial signals.

Characteristics. Organizations should identify the characteristics of the user's PNT system infrastructure and individual devices that provide, communicate, or consume PNT data. Characteristics of interest can include calibration to a traceable reference, PNT data stability over time, communication latency and jitter, and device response behavior at start-up under steady state conditions, with environmental stressors or disruptions, and typical observed PNT data characteristics.

Organizations should identify the environmental surroundings and conditions that the PNT system will be exposed to while maintaining the specified requirements. For example:

- Will there be sources of RF, multi-path interference?
- Will there be large temperature variations or extreme temperatures?
- Will there be sources of vibrations (e.g., along a busy road or in earthquake prone area)?

3.3.2 Detection of Disruptions to PNT Services

Editor's Note: *This section contains ways to detect disruptions to PNT services.*

System verification and validation policy and procedures. Organizations should identify steady state and transient test cases, test plans, and test schedules as an end user, applicable to the industry supply chain, to serve as a basis for verifying and validating PNT data users in order to manage assessed risks associated with PNT disruptions.

Spatial diversity and shielded antennas can be used to detect anomalies and possible spoofing. Other approaches include the use of diverse algorithms, cross-checking GPS solutions, verifying GPS data with other GNSS for consistency, and examining alternative constellations (low-earth orbit satellites, such as iridium) for sources of PNT.

It is beneficial to consider that the analysis and potential fusion of multiple and independent technologies can facilitate the detection of anomalies, improve the precision of PNT data, and ultimately contribute to a more resilient system in the event of a disruption.

There are numerous vendor products that detect anomalies using techniques such as analyzing the signal-to-noise ratio (SNR) or the doppler shift (on a per space vehicle basis).

3.3.3 Resilience of PNT Services

Editor's Note: *This section contains ways to operate through periods of PNT service outages or degradations.*

The ability to provide useable PNT data despite a compromise can be accomplished with technologies such as:

- Atomic clocks (with a known holdover)
- PNT diversity and segmentation
- Alternative signals, such as other satellite constellations
- Network-based solutions
- Terrestrial RF sources
- Signals of opportunity (such as cellular)

4 Conclusion

Editor's Note: *This section provides a brief conclusion to summarize the major points of the publication as well as discuss potential next steps and future work plans (e.g., communicating that this is a living document that will evolve over time).*

Appendix A—Acronyms and Abbreviations

Appendix B—Glossary

Appendix C—References

…

[EO 13636] Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/DCPD-201300091

[EO 13905] Executive Order 13905 (2020) Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services. (The White House, Washington, DC), February 12, 2020. https://www.govinfo.gov/app/details/FR-2020-02-18/2020-03337

[NIST CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

…

Appendix D—NIST Cybersecurity Framework

Editor's Note: *Appendix D summarizes the NIST Cybersecurity Framework (CSF), which provides guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.*

The NIST Cybersecurity Framework (CSF) provides guidance based on existing standards, guidelines, and practices to help organizations better manage and reduce cybersecurity risk. One component of the CSF – the Framework Core – describes a set of cybersecurity activities and desired outcomes determined to be essential across critical infrastructure sectors. The Framework Core consists of five concurrent and continuous Functions: Identify, Protect, Detect, Respond, and Recover. When considered together, these Functions provide a high-level, strategic view of the organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function and matches them with example Informative References, such as existing standards, guidelines, and practices for each Subcategory. The five Framework Functions can be performed concurrently and continuously to form an operational culture that addresses dynamic cybersecurity risk.

Table 1: Function and Category Unique Identifiers from NIST Cybersecurity Framework Version 1.1 [NIST CSF]

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

The five functions of the Framework Core are:

1. **Identify** – Develop organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities. The activities in the Identify Function are foundational to the effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to

focus and prioritize its efforts consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

2. **Protect** – Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impacts of a potential cybersecurity event. Examples of outcome Categories within this Function include Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.
3. **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable the timely discovery of cybersecurity events. Examples of outcome Categories within this Function include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.
4. **Respond** – Develop and implement the appropriate activities to respond to a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impacts of a potential cybersecurity event. Examples of outcome Categories within this Function include Response Planning, Communications, Analysis, Mitigation, and Improvements.
5. **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impacts of a cybersecurity event. Examples of outcome Categories within this Function include Recovery Planning, Improvements, and Communications.