NIST IR 8323r1 ipd

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

Initial Public Draft

Michael Bartock
Joseph Brule
Ya-Shian Li-Baboud
Suzanne Lightman
James McCarthy
Karen Reczek
Doug Northrip
Arthur Scholz
Theresa Suloway

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8323r1.ipd

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

# NIST IR 8323r1 ipd

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

Initial Public Draft


Michael Bartock
Suzanne Lightman
*Computer Security Division*
*Information Technology Laboratory*

Ya-Shian Li-Baboud
*Software Systems Division*
*Information Technology Laboratory*

James McCarthy
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Karen Reczek
*Standards Coordination*
*Office Laboratory Programs*

Joseph Brule
Doug Northrip
Arthur Scholz
Theresa Suloway
*The MITRE Corporation*
*McLean, VA*



This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8323r1.ipd

June 2022




U.S. Department of Commerce
*Gina M. Raimondo, Secretary*

National Institute of Standards and Technology
*Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology*

National Institute of Standards and Technology Interagency or Internal Report 8323r1 ipd
Initial Public Draft
136 pages (June 2022)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8323r1.ipd



**Public comment period:** June 29, 2022 – August 12, 2022

**Submit comments on this publication to:** pnt-eo@list.nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

All comments are subject to release under the Freedom of Information Act (FOIA).

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

## Abstract

The national and economic security of the United States (US) is dependent upon the reliable functioning of the nation's critical infrastructure. Positioning, Navigation, and Timing (PNT) services are widely deployed throughout this infrastructure. In a government wide effort to mitigate the potential impacts of a PNT disruption or manipulation, Executive Order (EO) 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation and Timing Services* was issued on February 12, 2020. The National Institute of Standards and Technology (NIST) as part of the Department of Commerce (DoC), produced this voluntary PNT Profile in response to *Sec.4 Implementation (a),* as detailed in the EO. The PNT Profile was created by using the NIST Cybersecurity Framework and can be used as part of a risk management program to help organizations manage risks to systems, networks, and assets that use PNT services. The PNT Profile is intended to be broadly applicable and can serve as a foundation for the development of sector-specific guidance. This PNT Profile provides a flexible framework for users of PNT to manage risks when forming and using PNT signals and data, which are susceptible to disruptions and manipulations that can be natural, manufactured, intentional, or unintentional.

## Keywords

critical infrastructure; Cybersecurity Framework; Executive Order; GPS; GNSS; navigation; PNT; positioning; risk management; timing.

## Supplemental Content

Any potential updates for this document that are not yet published in an errata update or revision—including additional issues and potential corrections—will be posted as they are identified; see the NISTIR 8323 publication details.

## Acknowledgments

The authors wish to thank all individuals, organizations, and enterprises that contributed to the creation of this document. A comprehensive acknowledgements section will be included in the final document.

## Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: pnt-eo@list.nist.gov

# Executive Summary

Executive Order 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing (PNT) Services*, was issued on February 12, 2020 [EO 13905]. It seeks to protect the national and economic security of the United States from the disruption or manipulation of systems that form or use PNT data and information vital to the functioning of U.S. critical infrastructure and technology-based industries. The Executive Order (EO) directs the Department of Commerce to develop a PNT Profile that will address the four components of responsible use of PNT, as stated in the EO:

1. Identify systems that use or form PNT data.
2. Identify PNT data sources.
3. Detect disruption and manipulation of the systems that form or use PNT services and data.
4. Manage risk regarding responsible use of these systems.

The PNT Profile provides a flexible framework for users of PNT services to manage risks when forming and using PNT signals and data, which are susceptible to disruptions and manipulations that can be natural, manufactured, intentional, and unintentional. It was created by applying the NIST Cybersecurity Framework (CSF) [NIST CSF] and can be applied to all organizations that use PNT services, irrespective of the level of familiarity or knowledge that they have with the NIST CSF. Organizations that have fully or partially adopted, or who have not adopted the NIST CSF can benefit.

The PNT Profile is voluntary and does not: issue regulations, define mandatory practices, provide a checklist for compliance, or carry statutory authority. It is intended to be a foundational set of guidelines. Sector-specific agencies (SSAs) and entities may wish to augment or further develop their own PNT cybersecurity efforts via full or partial implementation of the recommended practices in this document. Any implementation of its recommendations will not necessarily protect organizations from all PNT disruption or manipulation. Each organization is encouraged to make their risk management decisions in the context of their own cyber ecosystem, architecture, and components. The PNT Profile's strategic focus is to supplement preexisting resilience measures and elevate the postures of less mature initiatives.

# Table of Contents

## List of Appendices



## List of Figures



## List of Tables

# 1 Introduction

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 disruption or manipulation of positioning, navigation, and timing (PNT) services, particularly those organizations whose use of PNT services are vital to the functioning of U.S. critical infrastructure. EO 13905 directs the Department of Commerce to develop a PNT Profile for users of PNT services.

## 1.1 Purpose and Objectives

The PNT Profile is designed to be used as part of a risk management program in order to help organizations manage risks to systems, networks, and assets that use PNT services. The PNT Profile provides guidance for establishing risk management approaches to achieve the desired outcomes commensurate with acceptable and responsible levels of risk that result from the disruption or manipulation of PNT data. The PNT Profile is not intended to serve as a solution or compliance checklist that would guarantee the responsible use of PNT services.

Use of the PNT Profile will help organizations:

- Identify systems that use PNT services and determine their operating and performance requirements;
- Identify sources of PNT data;
- Identify known and anticipated threats to PNT services, equipment, and data;
- Protect systems that are dependent on PNT services by adhering to basic principles of responsible use;
- Detect disruptions and manipulation of PNT services and data;
- Address risk in the management and use of PNT services and data;
- Respond to PNT service or data anomalies in a timely, effective, and resilient manner; and
- Recover from PNT service or data anomalies in a timely, effective, and resilient manner.

## 1.2 Scope

The PNT Profile's scope includes systems that use PNT services, including 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]. PNT service providers include government systems, such as Global Positioning Systems (GPS), public NIST Network Time Protocol (NTP) servers, commercial services, and internal systems. The PNT Profile's scope does not include source PNT signal generators and providers (e.g., a Global Navigation Satellite System (GNSS) control segment or space segment, as shown in **Figure 1**).

PNT services interface with PNT systems and components operated by an organization to produce PNT data, which can take the form of position, navigation, or timing information. Responsible use of PNT services requires the stakeholder to identify the dependencies of PNT data (within their components, sub-systems, and systems), evaluate the impact should the disruption or manipulation of PNT data be

realized, and manage the residual risk.

This PNT Profile defines the responsible use of PNT services as it relates to critical infrastructure and national and economic security. In this case, responsible use by organizations includes incorporation of:

- Risk-informed management of PNT services;
- Risk-based approaches that minimize the potential effects of the disruption or manipulation of PNT services and data; and
- Deliberate planning and action regarding the secure management of PNT services

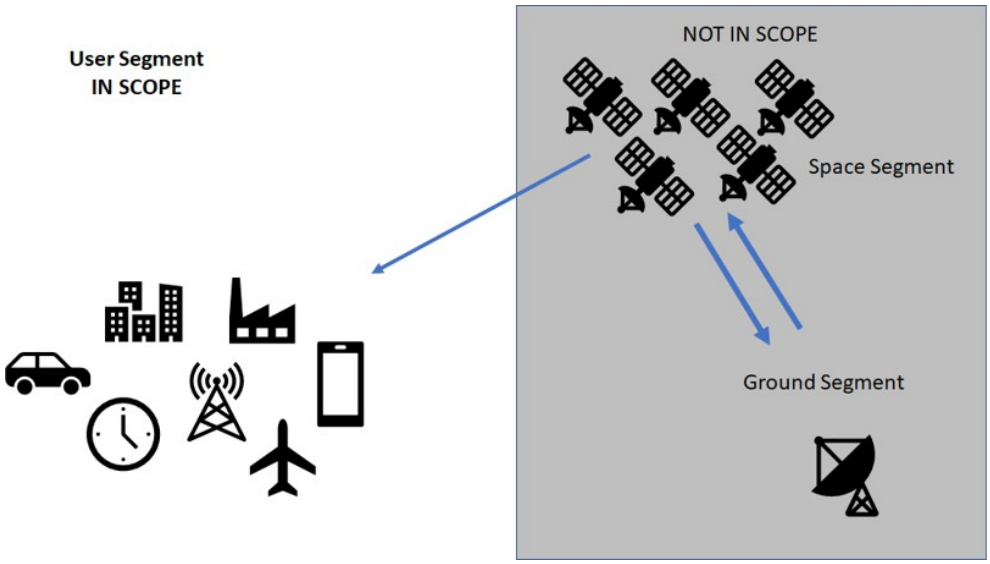



**Figure 1 - Example of How the PNT Profile Applies to GNSS**

The PNT Profile addresses systems and components operated by an organization to produce PNT data, which can take the form of position, navigation, or timing information. The provider (in this example, the GNSS space and ground segments) is not within the scope of the PNT Profile.

For the purposes of the PNT Profile, PNT data includes all information used by PNT equipment to form PNT solutions. This includes but is not limited to signals, waveforms, network packets, and other means to transmit PNT information.

## 1.3 Audience

This document's intended audience includes:

- Public and private organizations that use PNT services;
- Managers responsible for the use of PNT services;
- Risk managers, cybersecurity professionals, and others with a role in risk management for systems that use PNT services;
- Procurement officials responsible for acquisition of PNT services;
- Mission and business process owners responsible for achieving operational outcomes

dependent on PNT services; and
- Researchers and analysts who study systems that rely on PNT and/or study the unique cybersecurity needs of PNT services.

The PNT Profile is intended for a general audience and is broadly applicable. The PNT Profile applies to organizations that:

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

# 2 Intended Use

The PNT Profile is a flexible tool that can be used by an organization to help meet mission and business objectives that are dependent upon the use of PNT services. The PNT Profile can also help organizations determine risks based on their assessments of potential impacts of manipulation or disruption of PNT services to business and operational objectives. The PNT Profile is intended to help users of PNT services prioritize necessary cybersecurity activities based on business objectives. Additionally, the PNT Profile can be used to help organizations identify areas where standards, practices, and other guidance could help manage risks to systems that use PNT services. An organization can use the PNT Profile in conjunction with its systematic process for identifying, assessing, and managing risk. NIST acknowledges the existing efforts being undertaken by individual entities to address the responsible use of PNT services in their sectors. The PNT Profile is intended to complement, but not replace these efforts.

NIST also encourages the development of sector-specific guidance if more specific risk management efforts may be required. Organizations within various sectors can customize the PNT Profile by considering the following:

- What processes and assets require PNT data (direct recipients of PNT services)?
- What processes and assets are dependent on other assets that require PNT data (i.e., what are the secondary effects)?
- What processes and assets are vulnerable to the disruption or manipulation of PNT services?
- What are the integrity and availability thresholds of PNT to avoid mission impact?
- What safeguards are available?
- What is the impact to the organization should a process or asset be lost or degraded?
- What techniques can be used to detect events of concern?
- What techniques can be used to respond to events of concern?
- What techniques can be used to recover pre-event capabilities?

# 3 Overview

## 3.1 Risk Management Overview

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. An organization should also consider statutory and policy requirements that may influence or inform cybersecurity decisions.

The PNT Profile supports and is informed by cybersecurity risk management processes. Using the PNT Profile, organizations can make more informed decisions, based on business needs and risk assessments, 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 promote resiliency.

The PNT Profile provides a flexible approach for users of PNT to manage risks when forming and using PNT signals and data regardless of the source of the risk, including natural events, malicious actions, and human activities that have unintended consequences. It also provides a starting point from which organizations can customize their approach to manage risk to their PNT services and data. A customized approach provides the most appropriate measures, processes, and prioritization of resources for reliable and efficient functioning of critical infrastructure applications.

Organizations can use the PNT Profile in conjunction with existing risk management processes. The PNT Profile assumes that the organization implements cybersecurity risk management processes, and this profile is intended to provide additional risk management considerations specific to PNT. 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 list of additional resources is included in Appendix C of the PNT Profile.

## 3.2 Cybersecurity Framework Overview

Created through collaboration between industry and government, the Cybersecurity Framework [NIST CSF] provides prioritized, flexible, risk-based, and voluntary guidance based on existing standards, guidelines, and practices to help organizations better understand, manage, and communicate cybersecurity risks. Although it was designed for organizations that are part of the U.S. critical infrastructure, many other organizations in the private and public sectors (including federal agencies) use the NIST Cybersecurity Framework.

The NIST Cybersecurity Framework consists of three main components:[1]

1. The Framework Core provides a catalog of desired cybersecurity activities and outcomes[2] using common language. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.
2. The Framework Implementation Tiers provide context for how an organization views cybersecurity risk management. The Tiers help organizations understand whether they have a functioning and repeatable cybersecurity risk management process and the extent to which cybersecurity risk management is integrated with broader organizational risk management decisions.
3. The Framework Profiles are customized to the outcomes of the Core to align with an organization's requirements. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

The Framework Core presents standards, guidelines, and practices within five concurrent and continuous functions, which are described below. In the context of this "PNT Profile", a "cybersecurity event" refers to a potential for the disruption or manipulation of PNT services.

1. Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify function are foundational to the effective use of the NIST Cybersecurity Framework, enabling an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and business needs.
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 impact of a potential PNT cybersecurity event.
3. Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect function enable timely discovery of PNT cybersecurity events.
4. Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The activities in the Respond function support the ability to contain the impact of a potential PNT cybersecurity event.
5. Recover: Develop and implement the appropriate activities to maintain plans for resilience and to 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 impact of a PNT cybersecurity event.

[1] Elements of the Cybersecurity Framework—including Core, Implementation Tiers, Profile, Function, Category, and Subcategory—are normally capitalized and will be capitalized throughout this document.

[2] The word "outcomes" is used because the Cybersecurity Framework (CSF) focuses on the "what" rather than the "how." In other words, the emphasis is on the cybersecurity outcomes that the organization wants to achieve rather than how they will achieve it. The References described on page 8 help organizations with the "how."

When considered together, these functions provide a high-level, strategic view of the life cycle of an organization's management of PNT cybersecurity risk. The Framework Core then identifies underlying Categories and Subcategories for each Function. The 108 Subcategories are discrete cybersecurity outcomes that are organized into 23 Categories like "Asset Management" or "Protective Technology." **Table 1** shows the Five Functions and 23 Categories of the Core.

**Table 1 - Cybersecurity Framework Functions and Categories**

| 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 | 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 |

417

418 **References** are existing standards, guidelines, and practices that provide practical guidance to
419 help an organization achieve the desired outcome of each Subcategory. An example of two
420 Subcategories and applicable References within the Asset Management Category are shown in
421 **Figure 2**.
422

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| **IDENTIFY** (ID) | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | **ID.AM-1:** Physical devices and systems within the organization are inventoried | **CIS CSC** 1<br>**COBIT 5** BAI09.01, BAI09.02<br>**ISA 62443-2-1:2009** 4.2.3.4<br>**ISA 62443-3-3:2013** SR 7.8<br>**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2<br>**NIST SP 800-53 Rev. 4** CM-8, PM-5 |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | **CIS CSC** 2<br>**COBIT 5** BAI09.01, BAI09.02, BAI09.05<br>**ISA 62443-2-1:2009** 4.2.3.4<br>**ISA 62443-3-3:2013** SR 7.8<br>**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1<br>**NIST SP 800-53 Rev. 4** CM-8, PM-5 |

423 **Figure 2 - Cybersecurity Framework Subcategory Example**

424 The Subcategory outcomes are organized according to Functions and Categories and are not
425 prioritized within the Core. Each organization has unique requirements, risk tolerance and
426 resources. Therefore, the prioritization of the Subcategory outcomes will vary from one
427 organization to the next.

428 The PNT Profile in Section 3.3 can be used as a foundation for building a custom profile, as
429 shown in **Figure 3**. A custom profile can be built using the business objectives, threat
430 environment, requirements, and controls as inputs. The outcomes associated with a custom
431 profile based on the PNT Profile are the outcomes from the Executive Order: the identification of
432 systems dependent on PNT services that identify appropriate PNT services, detect the disruption
433 and manipulation of PNT services, and manage the risk to those systems.

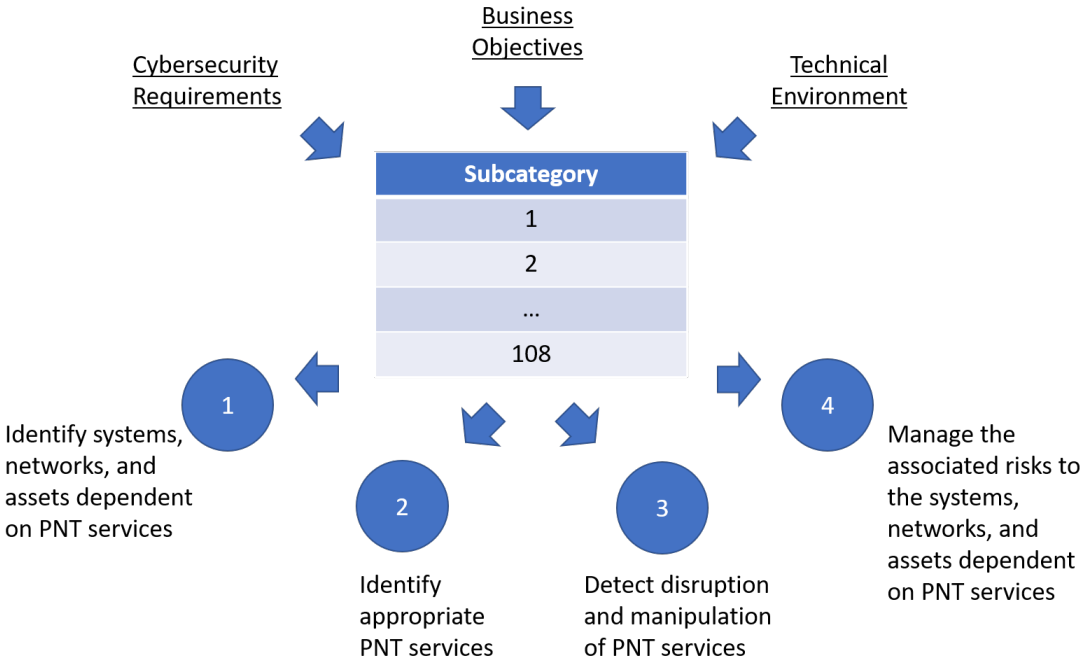



**Figure 3 - PNT Profile Creation Process**

Since organizations within the PNT community sector or sub-sector share many of the same business objectives and regulatory requirements, the creation of a high-level profile can provide a common starting point. The PNT Profile can make it easier for organizations to begin incorporating cybersecurity and can also be used to provide a baseline of cybersecurity for organizations within a sector or sub-sector. Individual organizations can further customize a profile by taking the sector/sub-sector profile and then tailor or augment it to address requirements, business objectives, or environmental threats unique to them.

The PNT Profile is intended to be implemented within the larger context of an organization that is developing and executing its own cybersecurity program.[3] That program should be based on organizational cybersecurity risk management policies and procedures. This PNT Profile is best implemented if a cybersecurity program is in place at the organizational level. However, this caveat does not preclude any organization from implementing the PNT Profile should a cybersecurity program not be in place.

[3] See IEC 62443 2-1, ISO/IEC 27001 (security management), and NIST SP 800-39.

# 4 The PNT Profile

This section was created by using the Cybersecurity Framework, as described in Section 3.2. The tables summarize the Subcategories for a Function and a Category. The references provided in the tables include cybersecurity guidance, PNT-specific guidance, and illustrative methods to implement the guidance. It is not intended to be a comprehensive list of all PNT references (see **References**), but a sample of potentially relevant resources depending on the PNT service(s) the organizations use and their PNT service and data requirements. The references that correspond to the Subcategory may not necessarily apply to all sectors. The Categories and Subcategories defined by the Cybersecurity Framework will address different aspects of the four components identified in the Executive Order, as illustrated in Table 2. Sections 4.1 through 4.5 provide insight on how the Subcategories address the responsible use of PNT. Note: Not all Subcategories in the NIST CSF are listed here; only those most applicable to this PNT Profile Acronyms described in the PNT Profile are listed in AppendixA.

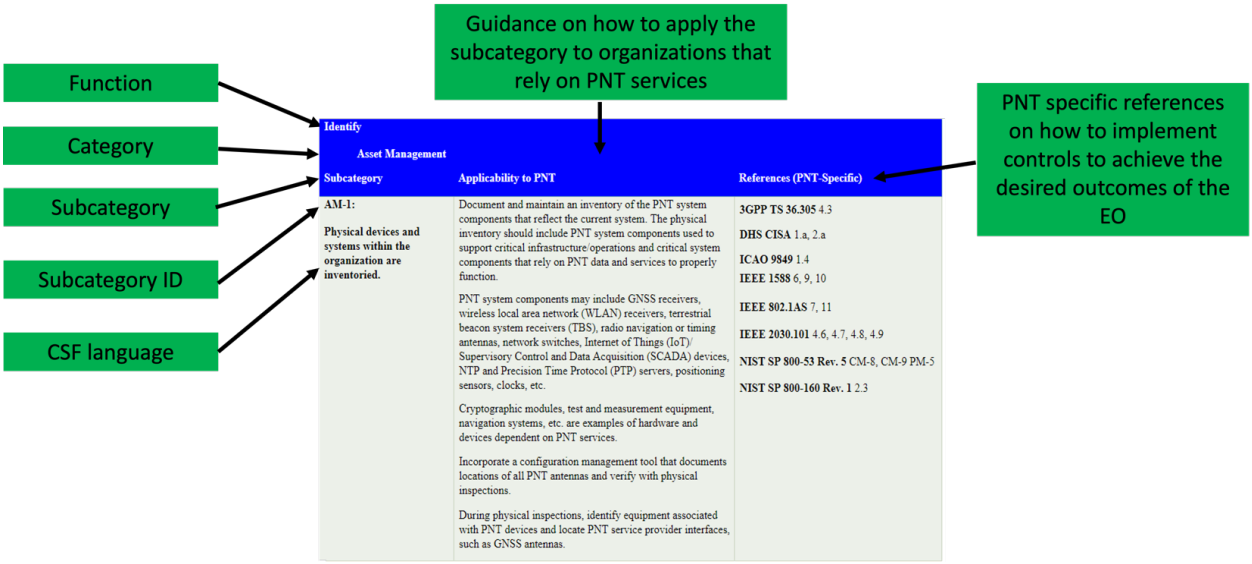
**Table 2 - Mapping the EO Implementation Guidance to the Cybersecurity Framework Profile**

| | | Identify systems dependent on PNT services | Identify appropriate PNT sources | Detect disturbance and manipulation of PNT services | Manage the risk to PNT systems |
|---|---|---|---|---|---|
| IDENTIFY | ASSET MANAGEMENT | X | X | X | X |
| | BUSINESS ENVIRONMENT | X | X | X | X |
| | GOVERNANCE | X | | | |
| | RISK ASSESSMENT | X | X | X | X |
| | SUPPLY CHAIN RISK MANAGEMENT | X | | X | X |
| PROTECT | ACCESS CONTROL | X | X | X | X |
| | AWARENESS AND TRAINING | X | | | |
| | DATA SECURITY | X | X | X | X |
| | INFORMATION PROTECTION PROCESSES AND PROCEDURES | X | X | | X |
| | MAINTENANCE | X | X | X | X |
| | PROTECTIVE TECHNOLOG Y | | X | X | X |

| | | Identify systems dependent on PNT services | Identify appropriate PNT sources | Detect disturbance and manipulation of PNT services | Manage the risk to PNT systems |
|---|---|---|---|---|---|
| DETECT | ANOMALIES AND EVENTS | X | | X | X |
| | SECURITY CONTINUOUS MONITORING | X | X | X | X |
| | DETECTION PROCESS | X | | X | X |
| RESPOND | RESPONSE PLANNING | | | | X |
| | COMMUNICATIONS | X | | | X |
| | ANALYSIS | | | X | X |
| | MITIGATION | | | X | X |
| | IMPROVEMENTS | | | | X |
| RECOVER | RECOVERY PLANNING | X | | X | X |
| | IMPROVEMENTS | X | | X | X |
| | COMMUNICATIONS | X | | X | X |

The Executive Order defines four components, and the NIST CSF defines a set of Functions and Categories. The PNT Profile maps the components of the Executive Order to the NIST CSF. It is important to note that there are interdependencies between the NIST CSF Functions and that each component of the Executive Order will require multiple Functions, Categories, and Subcategories.

Successful implementations require a comprehensive approach. The CSF Functions and guidance in the PNT Profile address the generic needs of PNT users in critical infrastructure that depend on PNT services to meet their business objectives. The components of the Foundational PNT Profile are concisely summarized in Figure 4 below. In order to support a risk-based, practical, and effective approach to the responsible use of PNT, organizations can select, tailor, and augment the security controls defined in PNT references in Sections 4.1 through 4.5.




475 **Figure 4 - Components of the PNT Profile**

## 4.1 Identify Function

The Identify function is foundational to the risk assessment process. It is highly recommended that those who intend to implement all or part of the PNT Profile start with the Identify function. An organization needs to analyze its mission objectives related to its reliance on PNT data.

The Identify function provides key activities that should be given strong consideration in this analysis. Consideration of the organization's mission and business objectives, threat environment, assets, and vulnerabilities will have a significant influence on the overall risk; these are directly addressed in the other four CSF functions (i.e., Protect, Detect, Respond, Recover).

The objectives of the Identify function include:

- Identify the business or operational environment and organization's purpose;
- Identify all assets, including applications dependent on PNT data;
- Identify sources and infrastructure that provide PNT information; and
- Identify the vulnerabilities, threats, and impacts should the threat be realized in order to assess the risk.

The Identify function within the NIST Cybersecurity Framework defines six categories, five of which have at least one subcategory that applies to the PNT Profile to varying degrees, as summarized in Sections 4.1.1 through 4.1.5.

### 4.1.1 Asset Management Category

The data, personnel, devices, systems, and facilities that enable the organization to achieve its business objectives are identified and managed in a manner that is consistent with their importance to organizational objectives and the organization's risk strategy. In the context of the PNT Profile, the assets that require and support PNT services in order to fulfill the organization's mission and business objectives are identified.

There are five subcategories within Asset Management that apply to the PNT Profile, as summarized in the table below.

501 **Table 3 - Identify – Asset Management Subcategories Applicable to PNT**

| **Identify**<br>**Asset Management**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **AM-1:**<br><br>**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.<br><br>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, clocks, positioning sensors such as Inertial Navigation Systems (INS), Inertial Measurement Units (IMU), proximity sensors, etc.<br><br>Cryptographic modules, test and measurement equipment, navigation systems, etc. are examples of hardware and devices dependent on PNT services.<br><br>Incorporate a configuration management tool that documents locations of all PNT antennas and verify with physical inspections. | **3GPP TS 36.305** 4.3<br><br>**DHS CISA** 1.a, 2.a<br><br>**ICAO 9849** 1.4<br><br>**IEEE 1588** 6, 9, 10<br><br>**IEEE 802.1AS** 7, 11<br><br>**IEEE 2030.101** 4.6, 4.7, 4.8, 4.9<br><br>**NIST SP 800-53 Rev. 5** CM-8, CM-9 PM-5<br><br>**NIST SP 800-160 Rev. 1** 2.3 |

| Identify<br>Asset Management<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| | During physical inspections, identify equipment associated with PNT devices and locate PNT service provider interfaces, such as GNSS antennas. | |
| **AM-2:**<br><br>**Software platforms and applications within the organization are inventoried.** | The software inventory should include PNT system components used to support critical infrastructure/operations and critical applications that rely on PNT data and services to properly function.<br><br>Document and maintain an inventory of PNT system software components, such as software license information, software version numbers, human-machine interface (HMI), and other industrial control systems (ICS) component applications, software, and operating systems. System software inventory is reviewed and updated as defined by the organization.<br><br>Identify all software, applications, and systems that are dependent on PNT data, including software that relies on distributed time, using phase and frequency synchronization methods. These methods may include packet-based communication protocols (e.g., NTP, PTP), frequency protocols using the physical layer network (e.g., Synchronous Ethernet (SyncE)), or physical signals (e.g., 10 MHz, 1 PPS, Inter-range instrumentation group time code B (IRIG-B)).<br><br>Applications dependent on PNT data may include test and measurement tools, kernels, databases, logging software, cryptography/certificate management, and other software that | **3GPP TS 36.305** 4.3<br><br>**DHS CISA** 1.a, 1.b, 1.c, 2.a<br><br>**DHS PNT** Appendix C<br><br>**ICAO 9849** 1.4, 5.1.4<br><br>**IEEE 1588** 5-14, Annex A, P<br><br>**IEEE 802.1AS** 7, 10<br><br>**IEEE 2030.101** 4.3<br><br>**IETF 5905** 5-15<br><br>**IETF 7384** 5, 7<br><br>**IMO 1575** Appendix C<br><br>**ITU-T G.8261** 6, 7, Annex A<br><br>**NIST SP 800-53 Rev. 5** CM-8, PM-5 |

| **Identify**<br>**Asset Management**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | rely on synchronized clocks or positioning information to verify information consistency. Some functions, such as multilateration, are also sensitive to timing performance, and should therefore be inventoried. | |
| **AM-3:**<br><br>**Organizational communication and data flows are mapped.** | Identify all connections within the PNT system, as well as between the PNT system and other systems. All connections and signal interfaces are documented, authorized, and reviewed.<br>Connection information may include the physical interface characteristics, logical interface characteristics, data characteristics, ports, port configurations, protocols, addresses, description of the data, security requirements, and nature of the connection.<br>Identify the PNT data source and distribution medium for the applications and systems that meets the PNT data performance and resilience requirements needed. It is critical to know where each system derives PNT data from. For example, the organization may want to investigate software programs that can help its organization identify PNT data sources to assess which sources are most beneficial to organizational mission stability. | **DHS CISA** 1, 2<br><br>**GPS IS-200** 3<br><br>**GPS IS-705** 3<br><br>**GPS IS-800** 3<br><br>**GPS SPS** B.1.2, B.1.3<br><br>**IEC 61850-90-4** 10, 14<br><br>**IEEE 1588** 8-12<br><br>**IEEE 802.1AS** 7.4, 8.5<br><br>**IEEE 2030.101** 4.2 |

| **Identify**<br>**Asset Management**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | For each software that provisions or uses PNT data, identify the input and output data interfaces. | **IETF 5905** 5-14<br>IMO 1575 **A-D, Appendix C**<br>ITU-T G.8261 **6**<br>ITU-T G.8262 **6-12, Appendix III**<br>**ITU-T G.8272** 6-12<br>**NIST SP 800-53 Rev. 5** AC-4, CA-3, CA-9, PL-8, SA-17<br>RTCA 326 **3.1.1**<br>**GAL ICD**<br>**BDS ICD** |
| **AM-4:**<br>**External information systems are catalogued.** | Identify and catalogue all external connections for the PNT system.<br>Identify all PNT signals, data sources, and related data products that pertain to an event or the status of the PNT source.<br>Examples of external systems include engineering design services and those that are controlled under separate authority, personal devices, and other hosted services. | **DHS CISA** 3<br>**NIST SP 800-53 Rev. 5** AC-20, PM-5, SA-9<br>USG FRP **Appendix B** |

| **Identify**<br><br>**Asset Management**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **AM-5:**<br><br>**Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.** | Determine required resources to support current regulations and standards requirements for the responsible use of PNT systems.<br><br>Provide adequate staffing with the appropriate training such that PNT support is available in a timely manner (consistent with thresholds defined in the organization's business plan). Formalize PNT roles and responsibilities to provide a process for transitioning staff members (with PNT expertise) to be replaced. The remaining staff members are provided with necessary resources and PNT training.<br><br>Identify and prioritize PNT system components, processors, and functions based on their classification, criticality, and business value.<br><br>Identify the types of information in the organization's possession, custody, or control for which security safeguards are needed (e.g., sensitive or protected information).<br><br>Stakeholders are advised to use other functions within the CSF to inform identification procedures. For example, while testing business continuity procedures, use the findings of a lost PNT source to identify which aspects of the mission were impacted and to what degree, and reprioritize accordingly.<br><br>When identifying resources and prioritizing trade-offs for PNT systems, holistically consider requirements, such as | **3GPP TS 22.071** 4<br><br>**DHS CISA** 3<br><br>**ISO/IEC/IEEE 15939:2017** 6.3.2.3<br><br>**NIST SP 800-37** 3<br><br>**NIST SP 800-53 Rev. 5** AC-20, RA-9<br><br>**USG FRP** Appendix B |

| Identify<br>Asset Management<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| | availability, continuity, data integrity, timeliness of anomaly detection, response, and recovery. | |

### 4.1.2 Business Environment Category

The organization's mission, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity roles, responsibilities, and risk management decisions. In the context of this PNT Profile, identify activities that are facilitated or require PNT services in order to fulfill the organization's mission, objectives, or other stakeholders' needs.

There are four Subcategories within Business Environment that apply to the PNT Profile, as summarized in the table below.

**Table 4 - Business Environment Subcategories Applicable to PNT**

| Identify<br>Business Environment<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| **BE-1:**<br><br>**The organization's role in the supply chain is identified and communicated.** | Organizations that engage in the reception and rebroadcast of PNT (or otherwise supply PNT) services to their consumers need to understand the cascading effects of a disruption or manipulation of PNT services to customers that may be a part of the critical infrastructure customers and rely on the PNT service. | **DHS S&T 2022**<br>**ISO/IEC 27001:2013**<br>**NIST SP 800-53 Rev. 5** CP-2, SR-3, SR-4<br>**NIST SP 800-37** |

| **Identify**<br><br>**Business Environment**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **BE-2:**<br><br>**The organization's place in critical infrastructure and its industry sector is identified and communicated.** | Critical infrastructure owner/operators need to understand and communicate the effects of a disruption or manipulation of PNT services on the organization's ability to fulfill its mission, objectives, or other stakeholders' needs.<br><br>Distribution of PNT data may rely on critical infrastructures such as power and communications sectors. For example, the accuracy of time and frequency transfer over fiber are sensitive to reflections, and users can benefit from fiber maintenance techniques that minimize reflections. | **DHS S&T 2022**<br>**NIST SP 800-53 Rev. 5** PM-11, RA-9<br>**NIST TN 2187** II.A.1 |
| **BE-4:**<br><br>**Dependencies and critical functions for the delivery of critical services are established.** | Identify and prioritize internal critical business services that are dependent on PNT system processes and components.<br><br>Identify any consumers and their requirements that rely on the organization's products or services whose delivery or production is derived from or relies upon PNT data. Recognize that different users and applications may have different requirements.<br><br>Identify and prioritize supporting services for critical PNT system processes and components.<br><br>For organizations that form PNT data, understand PNT data performance, the resilience levels of the service provided, and customer dependencies on PNT data. The organization's infrastructure, such as network communication architectures and protocols, can impact recovery time in the event of a path or node failure. | **DHS CISA** 3.a, 3.b, 3.c<br><br>**GPS** 2, 3, 4, 5<br><br>**GPS SPS** 3<br><br>**IEEE 2030.101** 4.4-4.7<br><br>**NIST SP 800-53 Rev. 5** CP-8, PE-9, PE-11, PM-8, RA-9<br><br>**USG FRP** 4, 6 |

| **Identify**<br><br>**Business Environment**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **BE-5:**<br>**Resilience requirements to support the delivery of critical services are established for all operating states (e.g. under duress or attack, during recovery, normal operations.)** | Consider and prioritize requirements in the context of safety, operational criticality, cost, and other resource availability.<br>operational criticality, cost, and other resource availability.<br>Identify performance levels of PNT data regardless of environmental threats or if applications can rely on alternatives without the PNT data (systems/components).<br>Define PNT data traceability requirements and reconcile with the PNT data performance (e.g., accuracy, integrity, continuity, availability, coverage) for the software, applications, systems, and environment in which the system<br>is operating.<br>Where applicable and practical, identify network performance parameters at the device's ingress and egress ports, static and dynamic delays between nodes, and end-to-end delay characteristics for the distribution of PNT data.<br>Resiliency requirements permit an organization to determine if the full capability of its current PNT service provider is needed. For example, if relative time synchronization or frequency synchronization is sufficient, then an organization may have more complementary holdover reference options.<br>PNT applications that require only a relative frame of reference may have additional resilience capabilities using local sensors, signals of opportunity, computations, and communications. | **3GPP TS 22.878** 4, 5<br>**DHS CISA** 6<br>**DHS PNT** III-V<br>**DHS RCF** 5-7<br>**GPS SPS** 3<br>**IEC 61850-90-4** 14.2.4<br>**IEEE 1588** 12.2<br>**IETF 8633** 3.2, 3.3<br>**ITU-T G.8262** 11<br>**ITU-T G.8272** 7<br>**ITU-T G.8275.1** Appendices I, II<br>**NIST SP 800-53 Rev. 5** CP-2, CP-11, RA-9, SA-8<br>**RTCA 229** 2.1.1.4, 2.1.2.3- 2.1.2.6, 2.1.3.3-2.1.3.6, 2.1.4.3- 2.1.4.7, 2.1.5.3 -2.1.5.7, 2.2.1.1, 2.2.1.2-2.2.1.6<br>**RTCA 235** 14.2, 14.3, 14.4<br>**USG FRP 1.7, 6** |

### 4.1.3 Governance Category

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. In the context of this PNT Profile, identify the legal, risk, environmental, and operational requirements that are enabled or impacted using PNT services.

There is one subcategory within Governance that applies to the PNT Profile, as summarized in the table below.

**Table 5 - Governance Subcategory Applicable to PNT**

| Identify<br>Governance<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| **GV-4:**<br><br>**Governance and risk management processes address cybersecurity risks.** | Develop a comprehensive strategy to manage risk to PNT-dependent operations. Include cybersecurity considerations in the risk management strategy. Review and update the risk management strategy, as necessary.<br><br>Understand governance structure, including quality assurance and oversight, of PNT sources, applications, and systems using PNT data for critical applications with respect to traceability, performance monitoring, and resilience requirements.<br><br>Implementations that include complementary or redundant PNT sources need to consider governance and risk implications, such as the interoperability, compatibility, and interchangeability of different sources. Verify that any impacts to the PNT data output are not detrimental to the mission. For example, understand how multiple GNSS constellations with different geodetic reference frames and time scales impact the PNT data output. GPS uses the WGS-84 geodetic reference frame, with errors less than 2 cm, for positioning. The average positioning | **DHS CISA** 2.b, 2.c, 3.a<br><br>**DOT CMPS**<br><br>**FCC E911**<br><br>**FINRA 4590**<br><br>**GPS GNSS**<br><br>**GPS IS-200** 3.3.4, 20.3.3.4.3.3.1<br><br>**ICAO 9849** 1, 6.2, 6.3, 7.2, 7.3, 7.15, 7.16<br><br>**IEEE 2030.101** Annex C<br><br>**Matsakis 2018**<br><br>**NIST SP 800-53 Rev. 5**, PM-3, PM-7, PM9, PM-10, PM-11, PM-28, RA-1, RA- |

| | | |
|---|---|---|
| | accuracy of GPS is within 8 m horizontal accuracy and within 13 m vertical accuracy. Centimeter-level GPS sensors are available for applications requiring higher accuracy. The GPS time scale is synchronized to UTC(USNO) within 1 µs, and typically within 30 ns (95 percentile) during normal operations<br><br>Be aware of legally accepted standards and sources. For example, UTC(NIST) and UTC(USNO) are the sources of legal time in the U.S. Depending on the time accuracy required USNO and NIST provide data products to support user traceability analysis.<br><br>Understand standards that support interoperability for PNT services and national/international coordination to support the performance, standardization, and cost minimization of user equipment.<br><br>Consider the governance and risk implications of using multi-GNSS receivers as well as practical considerations, such as interoperability and interchangeability of the different GNSS constellations for the organization's applications. Foreign PNT service providers, such as satellite constellations, should only be used in accordance with current federal policy guidance and restrictions. | 2, RA-3, SA-2<br><br>**NIST SP 800-160 Rev. 1** 3.3.8<br><br>**NIST USNO**<br><br>**RTCA 229** 1.3.3<br><br>**RTCA 326** 3.1.2<br><br>**USG FRP** 1.7.5 through 1.7.9, 6<br><br>**USNG**<br><br>**USNO GPS**<br><br>**GAL ICD**<br><br>**BDS ICD** |

### 4.1.4 Risk Assessment Category

The organization understands the cybersecurity risk to operations (including mission, functions, image, or reputation), assets, and individuals. In the context of this PNT Profile, the risk to organizational operations in the event of disruption or manipulation to PNT services is the main concern.

There are five Subcategories within Risk Assessment that apply to the PNT Profile, as summarized in the table below.

521 **Table 6 - Risk Assessment Subcategories Applicable to PNT**

| **Identify**<br><br>**Risk Assessment**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **RA-1:**<br><br>**Asset vulnerabilities are identified and documented.** | Identify, document, and report vulnerabilities that exist on the PNT system and the system that distributes PNT data. Where safe and feasible, include the use of vulnerability scanning on the PNT system, its components, or a representative system.<br><br>Testing and characterization to assess system vulnerabilities are recommended periodically or when there are changes to the threat model, the organization's reliance on PNT data, or modifications to the PNT equipment.<br><br>Receiver or system vulnerability testing may include PNT signal simulation to assess susceptibility to disruption or manipulation of the PNT signal. Testing should be conducted in accordance with industry best practices, laws, and regulations as well as within the business continuity constraints defined for the organization.<br><br>Vulnerabilities for an operational environment may include the susceptibility to atmospheric and scintillation effects on PNT signals, spoofing of unauthenticated signals, or disruptions or manipulations of PNT services. | **DHS CISA** 4.a<br><br>**DHS GPS CI**<br><br>**ICAO 9849** 5, 7.13<br><br>**IEEE 2030.101** 4.12, 4.14, 5<br><br>**NIST SP 800-53 Rev. 5** CA-2, CA-7, CA-8, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5<br><br>**NTP SEC**<br><br>**RTCA 229** 1.6.2, 2, 2.1.1.1.4, 2.1.1.1.5, 2.4, 2.5<br><br>**RTCA 356** 3.8.1, 3.8.2<br><br>**USG FRP** 1.7.3 |

| **Identify**<br><br>**Risk Assessment**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **RA-2:**<br>**Cyber threat intelligence is received from information-sharing forums and sources.** | Establish and maintain ongoing contact with security groups and associations to receive security alerts and advisories. Security groups and associations may include special interest groups, forums, professional associations, news groups, and peer groups of security professionals in similar organizations.<br><br>Implement a collaborative threat research and awareness program that includes a cross-organization information-sharing capability. Organizations should consider having both unclassified and classified information-sharing capabilities.<br><br>The coordination of information is important in building a comprehensive threat assessment indicator of evolving threats in the operating environment, including the geographical and temporal characteristics of the threat. | **DOT CGSIC**<br>**DHS CISA** 4.a<br>**ICS-CERT NCCIC**<br><br>**NERC EISAC**<br><br>**NTP SEC**<br><br>**NIST SP 800-53 Rev. 5** PM-15, PM-16<br><br>**USG FRP** Appendix B |

| | | |
|---|---|---|
| **RA-3:**<br><br>**Threats, both internal and external, are identified and documented.** | Threats in an operational environment may include natural, manufactured, intentional, and unintentional disruptions and manipulations, such as radio frequency interference (RFI), denial of service, data manipulation, unpredictable or uncharacteristic delays in the communication of PNT data, or loss of PNT service.<br><br>The threat assessment should include internal and external parties, user errors, hardware or software errors, compromise, failure, network impairments, and environmental conditions. Examples of threats to PNT data availability and integrity include (i) PNT user or component errors or impaired PNT components and communications; (ii) RFI, such as signal blockage, multipath, atmospheric scintillations, and interference from other radio frequency sources; (iii) other environmental threats, such as temperature variations, aging, vibrations, and power outages; (iv) hostile attacks, such as jamming, spoofing, High-Altitude Nuclear Detonation, High-Altitude Electromagnetic Pulse, or PNT component or network compromises (e.g., denial of service and delay attacks); and confidentiality, especially when PNT data is bound or associated with sensitive data. | **DIA**<br>**DOT 12464**<br>**DOT CGSIC**<br>**DHS GPS CI**<br>**GPS SPS** A.5.4.1<br>**ICAO 9849** 5.3- 5.5, Appendix F<br>**IETF 7384** 3<br>**IETF CMP** 6<br>**ITU-T 810** 6<br>**ITU-T GNSS** Appendix II, V, VII<br>**Kaplan** 9, 10<br>**NASIC**<br>**NIST SP 800-37** 2<br>**NIST SP 800-53 Rev. 5** PM-12, PM16, RA-3, SI-5<br>**NIST SP 800-160 Rev. 1** 2.3<br>**NOAA SWS**<br>**RTCA 235** 4-12<br>**RTCA 292** 2-14<br>**RTCA 326** 3.2<br>**RTCA 356** 3.2, 3.3, 3.4, 3.5 |
| **RA-4:**<br><br>**Potential business impacts** | The likelihood of an attack is a function of the capability and intent of a potential adversary that may be influenced by non-technical factors. For example, a foreign GNSS | **DOT 12464**<br>**IEEE 1139** |

| Identify<br><br>Risk Assessment<br><br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| **and likelihoods are identified.** | provider may deny PNT to the U.S. in a time of war or heightened tensions. Foreign satellite constellations should only be used in accordance with current federal policy guidance and restrictions.<br><br>Identify the potential business impacts of the disruption or manipulation of PNT service. The impact of a realized threat on PNT data performance and resilience may be evaluated in a test or field environment. Consider the impact of both observed and anticipated threats on downstream applications and users, as well as the potential interval of time during which the threat can continue. For each identified threat, include the extent of impact, error manifestation (step or ramp error and rate of ramp), detection thresholds, and error propagation implications on safety and operations.<br><br>Understand that the vulnerabilities for a system or component may impact dependent systems (i.e., a vulnerability may have impacts beyond the system that was subjected to an exploit). Based on applications' PNT data performance requirements, identify, characterize, and document the error sources of PNT data where applicable.<br><br>Documenting PNT measurement uncertainty characteristics in conjunction with the assessed vulnerability exploits is useful in order to assess whether the PNT data meets mission requirements. For example, time signals and data are subject to phase variations due to frequency drift, | **IEEE 1193**<br><br>**NIST SP 1065** 3-12<br><br>**NIST SP 800-53 Rev. 5** CP-2, PM9, PM-11, PM-9, RA-2, RA-3, RA-9<br><br>**NIST TN 1366**<br><br>**RTCA 235** 2.1,13<br><br>**RTCA 292** 2.3-2.6 |

| **Identify**<br><br>**Risk Assessment**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | frequency offset, jitter, wander, and discontinuities. Phase discontinuities can be caused by changes in the time source or in the network topology, where errors in signal regeneration or analog to digital conversion can contribute to performance degradation. | |
| **RA-5:**<br><br>**Threats, vulnerabilities, likelihoods, and impacts are used to assess risk.** | Conduct and document periodic assessments of risk to PNT systems that consider the threats, vulnerabilities, the likelihood that the threat will be realized, and the impact (including scale) to operations and assets.<br><br>The residual risk should be reassessed on a periodic basis, when there is a substantive change to the system's vulnerabilities (such as an equipment upgrade), a change in the likelihood of threat realization (such as a time of international tension), a change in the impact should a threat be realized (such as an organization's increased use or dependency on PNT services), or as a result of lessons learned from recovery actions.<br><br>The organization's failure and fault analysis should include all known threats to business processes due to a loss of PNT data assurance for a given operational environment.<br><br>Estimate the internal, external, environmental, intentional, and unintentional risks to the business or mission based the impact of a PNT disruption or manipulation. Consider the feasibility of continued operations. | **DHS GPS CI**<br><br>**ICAO 9849** 7.4, 7.5, Appendix F<br><br>**IETF 7384** 3.1-3.3<br><br>**IETF 8633** 3-9<br><br>**IETF 8915** 3-9<br><br>**IETF CMP**<br><br>**NIST SP 800-53 Rev. 5** CA-2, CA-7, PM-16, PM-28, RA-2<br><br>**NIST SP 800-160 Rev. 1** 2.3, 2.4<br><br>**RTCA 235** 2.1-2.4, 3, 14<br><br>**RTCA 326** 2.1, 2.2, 3.1- 3.4<br><br>**RTCA 356** 2.7, 3.5 |

### 4.1.5 Risk Management Strategy

The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions. The risk management strategy takes into consideration and factors all aspects of the organization (to include its reliance on PNT services). The responsible use of PNT (and associated assurance measures) will augment or influence the residual risk, definition of the priorities, identification of constraints and other aspects of the existing risk management strategy.

There are two subcategories in Risk Management that apply to the PNT Profile, as summarized in the table below.

| **Identify**<br><br>**Risk Management Strategy** | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT Specific)** |
| **RM-1:**<br><br>**Risk management processes are established, managed, and agreed to by organizational stakeholders.** | Responsible use of PNT services includes the consideration of the acquisition, integration, and deployment of PNT services. These considerations include the dependencies on the PNT primary sources and evaluation of the impacts as part of the PNT service acquisitions, systems integraton, and deployment. | **ISO/IEC 27001:2013**<br><br>**ISO / IEC / IEEE 15288 : 2015** 6.3.4<br><br>**ISO / IEC / IEEE 16085:** 2021 6, 7<br><br>**ISO 17666** 8.2, Annex A, B<br><br>**NIST SP 800-53 Rev. 5** PM-9<br><br>**NIST SP 800-37 Rev. 2** 3.1 |

| Identify | | |
|---|---|---|
| **Risk Management Strategy** | | |
| **Subcategory** | **Applicability to PNT** | **References (PNT Specific)** |
| **RM-3:**<br><br>**The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.** | The loss or degradation of an organization's capabilities or function may impact its customers, partners or other stakeholders. Residual risk analysis and subsequent risk management should consider impacts to external parties. This places the onus on the organization to determine its residual risk on factors beyond that of the organization; but it's impact as a critical infrastructure owner/operator within the sector.<br><br>The loss or degradation of an organization's capabilities or function may impact its customers, partners or other stakeholders. Consider and communicate the oeganization's risk tolerance to its stakeholders and its impact on critical infrastructure. | **ISO/IEC 27001:2013**<br><br>**NIST SP 800-53 Rev. 5** RA-9, PM-8, PM-9, PM-11 |

### 4.1.6 Supply Chain Risk Management Category

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks. In the context of this PNT Profile, identify the PNT service providers in order to assess and manage the risk to the PNT service.

There is one Subcategory within Supply Chain Risk Management that applies to this PNT Profile, as summarized in the table below.

**Table 7 - Supply Chain Risk Assessment Subcategory Applicable to PNT**

| **Identify**<br><br>**Supply Chain Risk Management**<br>Subcategory | **Applicability to PNT** | **References (PNT Specific)** |
|---|---|---|
| **SC-2:**<br><br>**Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.** | Identify any external systems or services that the organization uses for ingesting PNT data.<br><br>Remain apprised of current and future regulations related to the acquisition of PNT services, sources, and devices forming, transporting, or using PNT data.<br><br>Identify any external systems or services that the organization is dependent on for its PNT data.<br><br>In making supply chain decisions on PNT systems, components, and services, considerations may include (i) functional requirements; (ii) any relevant and applicable federal law, regulation, or statutory policy; (iii) the threat environment; (iv) mission-level goals, criticality, and functions; (v) security policies; (vi) organizational policies, vulnerabilities, | **DHS GPS CI** 5<br><br>**NDAA** 889<br><br>**NIST SP 800-161** 2.2, 3<br><br>**NIST SP 800-53 Rev. 5** PM-9, RA-3, SR-2, SR-3, SR-5, SR-6<br><br>**USG FRP** 1.7 |

| | | |
|---|---|---|
| | risks, and risk tolerance; and (vii) the business objectives.<br><br>Supply chain vulnerabilities include (i) systems and components; (ii) the development and operational environment; and (iii) the logistics or delivery environment that transports systems and components (logically or physically). Consider access paths within the supply chain that would allow adversaries to gain information about the PNT system and introduce hardware, software, or firmware that could cause the disruption or manipulation of the PNT data as well as any dependencies that may be easier to subvert.<br><br>Supply chain threat sources include (i) hostile cyber or physical attacks to either the supply chain or an information system component traversing the supply chain; (ii) human errors; and (iii) geopolitical disruptions, economic upheavals, and natural or manufactured disasters.<br><br>Likelihood determination of PNT supply chain exploits include (i) threat information and assumptions; (ii) PNT component exposure to external access; (iii) system, process, or component vulnerabilities; and (iv) empirical data on vulnerabilities from system, process, and component test and analysis results.<br><br>Mission criticality and impact analysis of supply chain vulnerabilities, threats, and likelihood of PNT systems and components can be used to determine the organization's risk and guide the selection of supply chain security controls. | |

## 4.2 Protect Function

The Protect Function includes development, implementation, and verification measures to prevent the loss of functionality in the case of PNT disruption or manipulation. Additionally, the Protect function enables the response to and recovery from cybersecurity events with planning and preparation activities, while the execution of risk mitigation is addressed in the Response and Recovery functions.

The objectives of the Protect function include:

- Protect the systems that form, transmit, and use PNT data to support the needed level of integrity, availability, and confidentiality based on application needs.
- Protect the deployment and use of PNT services through adherence to cybersecurity principles, including understanding the baseline characteristics and application tolerances of the PNT sources, data, and any contextual information; providing sufficient resources; managing the systems development life cycle (SDLC); and deploying needed training, authorizations, and access control.
- Should a threat be realized, protect users and applications that are dependent on PNT data by enabling them to maintain a sufficient level of operations through verified response and recovery plans.
- Protect organizations that rely on PNT services and data with respect to business and operational needs.

The Protect function defines six categories, all of which have at least one subcategory that applies to this PNT Profile in varying degrees, as summarized in Sections 4.2.1 through 4.2.6.

### 4.2.1 Access Control Category

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities. In the context of this PNT Profile, assets may include GNSS antennas, receivers, servers, and subscriptions, and “physical access” may include radio frequency emanations.

There are seven subcategories within Access Control that apply to this PNT Profile, as summarized in the table below.

558 **Table 8 - Protect Access Control Categories Applicable to PNT**

| Protect<br>Access Control<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| **AC-1:**<br><br>**Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.** | Where applicable, establish and manage identification and authentication credentials of PNT users, data sources, and applications that use PNT data.<br><br>When warranted, authenticate PNT sources and data to verify PNT data integrity. Authentication can also be used to verify that PNT resources are used by authorized devices, users, and processes.<br><br>Revoke credentials when the authorization of PNT sources, devices, users, and processes expires or is no longer needed. | **DHS GPS CI**<br><br>**DHS TFS** 3.10, 3.11<br><br>**IEEE 1588** Annex P 2.1.2<br><br>**IETF 5906** 7, 8, 10<br><br>**IETF 7384** 5.1<br><br>**IETF 8915** 1, 5.2, 5.6, 5.7, 8<br><br>**NIST SP 800-53 Rev. 5** IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-10, IA-11, IA-12 |
| **AC-2:**<br><br>**Physical access to assets is managed and protected.** | Protect physical access to the PNT equipment and resources. Determine access requirements during emergency situations.<br><br>Maintain and review visitor access records to the facility where the PNT equipment resides, including antennas.<br><br>The access and provisioning process may include lists of authorized individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, and the monitoring of facility access. For example, obscure the visibility of antennas from public access, or use decoy antennas. | **DHS GPS CI**<br><br>**NIST SP 800-53 Rev. 5** PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9 |

| **Protect**<br>**Access Control**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| AC-3:<br><br>Remote access is managed. | Establish usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the systems that use or form PNT data.<br><br>Consider radio frequency as part of remote access and employ appropriate mitigations at the receiving antennae.<br><br>Enable secure remote access and management to PNT systems and devices. Compliance to secure standardized network management protocols can facilitate remote network management and monitoring.<br>Ensure safe use of service and management protocols by following security alerts and adhering to latest best practices. Document the use of security capabilities, such as access control lists, authentication, and configuration parameters to reduce the probability of cyberattacks. | **DHS GPS CI**<br><br>**DHS TFS** 3.11<br><br>**IETF CMP** 1, 4, 6<br><br>**IEEE 1588** Annex P 2.5.3<br><br>**IETF CMP** 3-6<br><br>**NIST SP 800-53 Rev. 5** AC-1, AC-17, AC-19, AC-20, SC-15<br>**SNMP3 SNMPSEC** |
| **AC-4:**<br><br>**Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.** | Create access control lists that enforce which authenticated users are authorized to use or perform actions on PNT systems.<br><br>Enable approved access lists for all controls that follow, such as NTP and PTP time servers, signaling channels, and other PNT systems.<br><br>Define and manage access permissions for systems that use PNT services. Identify user actions that can be performed on the systems that use or form PNT data without needing to verify identification or | **IEEE 1588** Annex P 2.1.2, 2.5.2, 2.5.5<br><br>**IETF 8633** 3.4, 5.1<br><br>**NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC5, AC-6, AC-14, AC-16, AC-24<br><br>**NIST SP 800-160 Rev. 1** Appendix F.1.14 |

| Protect<br><br>Access Control<br><br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| | authentication (e.g., during emergencies). | |
| **AC-5:**<br><br>**Network integrity is protected (e.g., network segregation, network segmentation).** | Identify and control connections between system components. Monitor and control connections and communications at the external boundary and at key internal boundaries.<br><br>Information Assurance (IA) measures to ensure integrity should be considered at the network boundaries and internal controls. Boundary protection mechanisms may include boundary clocks, routers, gateways, unidirectional gateways, data diodes, and separating system components into logically separate networks or subnetworks. Intradomain measures include network segmentation and segregation where appropriate.<br><br>Consider the isolation of control plane, user plane, and signaling plane where appropriate and practical. | **DHS CISA** 1.a, 4.a<br><br>**IEEE 1588** Annex P<br><br>**IETF 5906** 6<br><br>**IETF 7384** 5.2<br><br>**NIST SP 800-53 Rev. 5** AC-4, SC-7, SC-10 |
| **AC-6:**<br><br>**Identities are proofed and bound to credentials and asserted in interactions.** | Prior to issuing identity credentials and authorizations to form or to use PNT data, determine the identity and any associated contextual information needed about a user, device, or process to establish a satisfactory level of assurance. Contextual information used to proof user or asset identity may include proximity, location, movement, associations, and environmental factors.<br><br>PNT data sources are validated for authenticity. | **ATIS-I-0000070** 2-7<br><br>**DHS CISA 2.d**<br><br>**DHS GPS CI**<br><br>**IEEE 1588** 16.14, Annex P<br><br>**IETF 5906** 7, 8-10<br><br>**NISTIR 8014** 4-6 |

| **Protect**<br><br>**Access Control**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | Clients, applications, and systems are validated for the authorized use of the PNT data or services.<br><br>Note that the sensitivity (and associated confidentiality requirements) of PNT data may be impacted when bound or associated with other data. | **NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12,<br><br>PE-2, PS-3 |
| **AC-7:**<br><br>**Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).** | Ensure that PNT devices and equipment use appropriate authentication for the risk associated with downstream operations, which depend on accurate and reliable PNT data. Not all PNT services support authentication, and alternates should be sought when practical and warranted.<br><br>Users, devices, and assets are authenticated to prevent the realization of cyberthreats via remote connections to the PNT data source.<br><br>Authentication protects data provenance and verifies the authenticity of the data source. Implement source, client, or mutual authentication based on the IA requirements of the organization and be cognizant of the fact that different applications may have different authentication requirements.<br><br>Understand that implementations may influence message delay and delay variations. Verify that PNT data performance remains within tolerances. | **DHS CISA** 2.d, 5.b<br><br>**DHS GPS CI**<br><br>**DHS TFS** 2.2<br><br>**IEEE 1588** 16.14, Appendix P.2.1, 2.2<br><br>**IETF 4082** 2-5<br><br>**IETF 5906** 2-12<br><br>**IETF 7384** 5.1, 5.7<br>**IETF 7822** 2-4<br><br>**IETF 8573** 3-7<br><br>**IETF 8633** 5.5, 5.6<br><br>**IETF 8915** 1,4, 5.5, 8.3, 8.4<br><br>**NIST NTP**<br>**NIST SP 800-53 Rev. 5** AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11 |

### 4.2.2 Awareness and Training Category

The organization's personnel and partners are provided cybersecurity awareness education and trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. In the context of this PNT Profile, the focus is on privileged users who monitor and maintain equipment that forms, communicates, or uses PNT data.

There are two subcategories within Awareness and Training that apply to the PNT Profile, as summarized in the table below.

565 **Table 9 - Awareness and Training Subcategory Applicable to PNT**

| **Protect**<br><br>**Awareness and Training** | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
| **AT-2:**<br><br>**Privileged users understand their roles and responsibilities.** | Determine how to establish what privileged user qualifications are, what training is required to meet those qualifications, and ways to validate that the qualifications have been met.<br><br>Consider comprehensive training programs for transitioning staff assigned to the business and operational implementation of the organization's PNT services and applications that are dependent on PNT data. Operators, network and system administrators, and other technical staff are trained to install, test, and maintain PNT systems, as well as to detect and respond to compromised PNT data with respect to the PNT data source and applications or systems that use PNT data. | **DHS CISA** 5.a<br><br>**ICAO 9849** 1.3.1, 1.3.4, 7.3, 7.4, 7.5.6, 7.6.1<br><br>**NIST SP 800-53 Rev. 5** AT-3, PM-13<br><br>**NIST SP 800-160** Appendix E<br><br>**USG FRP** 1.7.8 |
| **AT-3:**<br><br>**Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.** | Applicable to organization that consume and rebroadcast PNT services and organizations that produce PNT related hardware to the critical infrastructure. Owners and operators would include this sub-category for third party contracting requirements.<br><br>Identify and communicate user boundaries and responsibilities for monitoring, control, and assuring performance tolerances of PNT data. | **DHS S&T 2022**<br><br>**ISO/IEC 27001:2013**<br><br>**NIST SP 800-53 Rev. 5 PS-7, SA-9, SA-16**<br><br>**NIST TN 2187** II.A.4 |

### 4.2.3 Data Security Category

Information and data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of PNT services. In this PNT Profile, the availability and integrity of PNT services are of primary concern throughout the enterprise. PNT data that is bound or associated with personally identifiable information (PII) or other sensitive data increases confidentiality concerns.

There are seven subcategories within Data Security that apply to the PNT Profile, as summarized in the table below.

**Table 10 - Data Security Subcategories Applicable to PNT**

| **Protect**<br>**Data Security**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **DS-1:**<br>**Data at rest is protected.** | Applications dependent on PNT data, such as location and time stamp to log the position and time of an event, may need to protect against repudiation and alteration. Sensitive information may need to be encrypted.<br><br>PNT data may be critical for downstream activities, such as analytics and forensics. Apply measures such as access control lists, encryption, and other data-at-rest protections commensurate with the criticality of the activities dependent on PNT. | **GPS ICD-870** 3.3, 3.3.1<br>**IETF CMP** 6<br>**NIST SP 800-37** 3<br>**NIST SP 800-53 Rev. 5** MP-3, MP-4, MP-6, SC-28 |

| **Protect**<br>**Data Security**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **DS-2:**<br>**Data in transit is protected.** | Use encryption and transmission security in accordance with availability, integrity, and confidentiality requirements. Time protocols may need integrity, authentication, and—for certain use cases—confidentiality protections. Prior to deploying encryption or decryption implementations, understand the implementation's effects on PNT data communications delay and delay variances. Verify that synchronization precision remains within the specified tolerances. | **IEEE 1588** 16.14, Annex P.2.2.1.3, P.2.2.3<br>**IETF 7384** 5.1-5.3, 5.7-5.9<br>**IETF 8915** 1, 3-9<br>**IETF NTS** 1-10<br>**NIST SP 800-53 Rev. 5** SC-8, SC-11, SC-12 |
| **DS-3:**<br>**Assets are formally managed throughout removal, transfers, and disposition.** | Depending on the assessment of the sensitivity of PNT data, enforce accountability for all PNT system components throughout the system life cycle, including removal, transfers, and disposition.<br>Some of the asset management requirements can be met by implementing solutions that provide the hardware inventory, software inventory, systems development life cycle management, and media sanitization technical capabilities. | **DHS CISA** 4.b<br>**ISO/IEC 15288:2015**<br>**NIST SP 800-53 Rev. 5** CM-8, MP-6, PE-16, PE-20 |
| **DS-4:**<br>**Adequate capacity to ensure availability is maintained.** | Provide enough capacity to meet PNT data performance requirements—including availability, stability, and timeliness—and verify that the capacity will perform within predefined thresholds under normal operating conditions as well as in the presence of PNT service disruptions and manipulation. Consider performing developmental and operational tests to verify and validate PNT service performance under normal and contested conditions. | **3GPP TR22.878** 4, 5<br>**3GPP TS36.305** 4.3<br>**DHS RCF** 3, 5.3, 5.4<br>**DHS PNT** IV, V<br>**GPS GNSS**<br>**ICAO 9849** 2.2.3, 2.2.4, 5.1, 6.2, Appendix |

| **Protect**<br>**Data Security**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | Consider the principle of defense in depth using independent, diverse, and isolated PNT sources and communication paths. For example, multi-GNSS and multi-frequency receivers may mitigate interference events and spoofing attacks, as well as avoid errors due to variations in ionospheric delays. However, foreign satellite constellations should only be used in accordance with current federal policy guidance and restrictions.<br>Keep apprised of potential and scheduled disruptions from PNT service providers.<br>Where needed, incorporate measures such as stand-alone and holdover capabilities or other means for deriving PNT data when PNT sources are unavailable. | G<br>**IEC 62439-3** 4, 5<br>**IEEE 1588** Appendix P.2.3<br>**IEEE 2030.101** 4.6, 4.8, 4.9, 4.12, 4.13<br>**IETF 7384** 5.4<br>**ITU-T G.8262** 11<br>**ITU-T G.8275** 7.2<br>**Kaplan** 1.8, 12, 13<br>**NIST SP 800-53 Rev. 5** AU-4, CP-2, PE-11, SC-5<br>**NIST SP 800-160** Appendix F.4<br>**RTCA 229** 1.5.2, 2.1.1.7- 2.1.1.9, 2.1.2.3- 2.1.2.6, 2.1.3.7- 2.1.3.9, 2.1.4.7- 2.1.4.9, 2.1.5.7- 2.1.5.9, 2.5.9.2<br>**RTCA 356** 3.5, 5.6.1<br>**USG FRP** 1.7.5.2, 6 |

| **Protect**<br>**Data Security**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **DS-5:**<br>**Protections against data leaks are implemented.** | Protect the PNT system against data leaks. Special attention must be paid to PNT data which is bound to or used in conjunction with potentially sensitive data, such as PII.<br>The physical location of critical assets needs to be protected against data leaks. | **IETF 8633** 5.1<br>**IETF 8915** 1, 9<br>**NIST SP 800-53 Rev. 5** AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4, |
| **DS-6:**<br>**Integrity-checking mechanisms are used to verify software, firmware, and information integrity.** | Implement methods to verify integrity in the event of PNT data discrepancies among PNT sources.<br>Protections should also be put in place to verify that PNT input signals conform with service interface specifications and prevent internal data corruption.<br>Information integrity may be checked or verified using redundant or independent PNT sources. Methods to evaluate PNT data integrity include algorithms that check the consistency of PNT output data and estimate the current magnitude and characteristics PNT data errors and uncertainty. For example, using multiple GNSS frequencies and multiple constellations can provide a means to cross- check PNT data and potentially remove error sources. However, foreign satellite constellations should only be used in accordance with current federal policy guidance and restrictions. Be aware of the potential for PNT data ambiguities in the PNT system and prepare users and applications to resolve any potential ambiguity | **3GPP TS36.305** 4.3<br>**DHS CISA** 2.c<br>**DHS GPS CI** 3<br>**DHS RCF** 5.2, 7, 8<br>**DHS S&T**<br>**GPS GNSS**<br>**GPS IS-200**<br>**GPS IS-705**<br>**GPS IS-800** 3<br>**GPS ICD-240**<br>**GPS ICD-870**<br>**ICAO 9849** 2.2.2, 4.1-4.4, 7.8, 7.10<br>**IEEE 1139**<br>**IEEE 1193** |

| **Protect**<br>**Data Security**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | (when two or more PNT systems disagree).<br>Consider PNT systems that employ authentication and encryption of PNT data to preserve integrity and resist spoofing.<br>Consider using an ensemble of multiple PNT sources to improve PNT data integrity and to estimate data uncertainties.<br>Consider using PNT receivers that can verify that the data has been produced by a trusted identity and has not been modified.<br>Consider PNT receivers that execute data integrity checks and IS/ICD/Data compliance checks to verify integrity and resist spoofing.<br>Qualify new PNT firmware and software by verifying, validating, and executing documented device and end-to-end test plans under normal and failure mode conditions, and can include but not limited to standards conformance and interoperability testing.<br>Consider including potential PNT data interoperability issues in the affected application systems validation test plan, including leap second and GPS week rollover testing, well in advance of an event.<br>For critical systems, consider verifying and validating PNT systems, components, and procedures through tests, | **IEEE 1588** 16.14, Annex P 2.2<br>**IEEE 2030.101** 5<br>**IETF 5906** 4<br>**IETF 8633** 3.7, 4<br>**IETF 8915** 1, 5<br>**IMO 1575** Appendix C<br>**ISO/IEC 17025**<br>**NIST SP 800-53 Rev. 5** SI-7, SI-10<br>**NIST SP 800-160 Rev. 1** 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F<br>**RTCA 229** 1.6, 1.8.1.5, 2.1.1.1- 2.1.1.6, 2.1.1.10, 2.1.1.12, 2.1.2.1, 2.1.2.2, 2.1.3.1,2.1.3.2, 2.1.4.1, 2.1.4.2, 2.1.4.10, 2.1.4.11, 2.1.5.2, 2.2.1.6, 2.5.8, 2.5.9<br>**US FRP** 1.7, 4.3, A.1.10<br>**GAL ICD**<br>**BDS ICD** |

| Protect<br>Data Security<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| | measurements, inspections, and continuous monitoring. | |
| **DS-8:**<br>**Integrity checking mechanisms are used to verify hardware integrity.** | Verify PNT device calibration, status, orientation (e.g., antenna positioning), and actual state compared to the desired state.<br>Consider standards-based mechanisms, such as Trusted Platform Modules (TPM) and other device attestation measures when warranted and practical. | **DHS GPS CI** 4, 6<br>**IEEE 1588** Annex M, N<br>**NISTIR 8320**<br>**NIST SP 800-53**<br>**Rev. 5** PE-11, SA-10, SI-7 |

### 4.2.4 Information Protection Processes and Procedures Category

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets. In the context of this PNT Profile, the PNT data and services are subject to the security policies of the information that the PNT data is bound or associated with (e.g., PII, location of critical assets).

There are five subcategories within Information Protection Processes and Procedures that apply to the PNT Profile, as summarized in the table below.

580 **Table 11 - Information Protection Processes and Procedures Applicable to PNT**

| **Protect**<br>**Information Protection Processes and Procedures** | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
| **IP-1:**<br><br>**A baseline configuration of information technology / industrial control systems is created and maintained that incorporates security principles (e.g. concept of least functionality) is created and maintained.** | Document baseline information for PNT devices and components (e.g., serial numbers, license information, version numbers, HMI and other ICS component applications, patch information). Document configuration instructions and backups, architecture and wiring diagrams, and other PNT system information so that the reliance on and interdependency of PNT-related assets are understood and can be maintained.<br><br>Install and configure PNT devices and components per manufacturer instructions using established safety and best practices guidelines. Understand the limitations of the original equipment manufacturer (OEM) equipment being fielded and consider the ability of the PNT devices and components to be suitable for the site's environment and adaptable to new features and protection mechanisms for PNT data.<br><br>Periodically review and simplify PNT systems to reduce unknown interactions and effects. Configuring the PNT devices and components in a manner such that only essential capabilities are provided can reduce complexity and may reduce the attack surface. Network configuration and deployment can impact recovery time in the event of a path or node failure.<br><br>Verify that the baseline configuration results in a system | **3GPP TR22.878** 4, 5<br>**DHS CISA** 4.b, 5.b<br>**DHS GPS CI** 11<br>**DHS TFS** 1, 2<br>**GPS-SPS** 2.4<br>**ICAO 9849** 6.4, Appendix F 5.2, 5.3<br>**IEEE 1588** Annex P<br>**IEEE 2030.101** 4.6-4.13, 4.15<br>**IETF 5906** 5<br>**IETF 8633** 2-9<br>**IMO 1575** C.1, E<br>**ITU G. 8272** I.1<br>**ITU-T G.8275** 7, 8<br>**ITU-T GNSS** 2, 4, 5, Appendix V, VII<br>**NIST SP 800-53 Rev. 5** CM-1, CM-2, CM-3, CM-4, CM5, CM-6, CM-7, CM-9, SA-10<br>**NIST SP 800-160** 3.4.9, 3.4.10, 3.4.11 Appendix F, G |

| **Protect**<br>**Information Protection Processes and Procedures**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | that meets the baseline PNT performance requirements, such as uncertainty, wander, and jitter tolerances. | **NTP SEC**<br>**RTCA 229** 2.2.1.1, 2.4.1, 2.5.2, 2.5.3, 2.5.4, 2.5.7, 2.5.11<br>**RTCA 235** 2.5.2.1, 2.5.2.2, Appendix G<br>**RTCA 356** 3.5, 3.6, 5.6.1, 5.6.4, 5.6.5<br>**USG FRP** Appendix A |
| **IP-2:**<br><br>**A System Development Life Cycle to manage systems is implemented.** | An operational system development life cycle for PNT services is established to incorporate and manage security measures throughout the life cycle of components.<br>Document the requirements, approach, architectures, and assumptions used to minimize risks for systems that form or use PNT data, thereby verifying PNT data performance, such as the availability, integrity, and confidentiality of services.<br>Consider the intended lifetime of the systems that form PNT data. The system components and architecture should be designed for complementary or redundant PNT sources to mitigate end-of-life and reliability issues, limit the failure modes, and increase the probability that the organization's PNT systems are able to detect anomalous inputs and remain available through the presence of different threat models.<br>Select, use, and ensemble complementary PNT services based on system priority classifications to meet business | **DHS CISA** 4.b<br>**IEEE 2030.101** 4.5, 4.6<br>**NIST SP 800-53 Rev. 5** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17<br>**NIST SP 800-160 Rev. 1** 3.2.1, Appendix F.3<br>**RTCA 326** 4.2<br>**USG FRP** 1.4, 1.7.2 |

| **Protect**<br>**Information Protection Processes and Procedures**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | continuity objectives. | |
| **IP-3:**<br>**Configuration change control processes are in place**. | Employ configuration change control for PNT devices and components that are consistent with the software development life cycle to maintain a functioning baseline and monitor all changes to validate impacts and integrity.<br>Prior to deploying a change, conduct impact analyses. Identify and record the effects of impact on downstream applications, users, and downtime.<br>Provide a mechanism so that changes in PNT firmware and software can be returned to a proper working state and should comply with the latest standards.<br>Change control and maintenance procedures should include documentation and artifacts that will impact the performance of the PNT system, such as calibration procedures. | **DHS GPS CI**<br>**IMO 1575** C.1, E.3<br>**NIST SP 800-53 Rev. 5** CM-3, CM-4, SA-10<br>**NIST SP 800-160 Rev. 1** 3.3.5<br>**RTCA 356** 3.8.3, 3.8.4 |
| **IP-9:**<br>**Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.** | Develop and maintain response and recovery plans that identify essential functions and associated contingency requirements, as well as provide a roadmap for implementing incident response. Plans should incorporate recovery objectives, such as the practical resilience level of the PNT system, restoration priorities, tests, metrics, contingency roles, personnel assignments, and contact information. Prioritize maintaining essential functions despite system disruption or manipulation, as | **DHS CISA** 1.f<br>**DHS IDM**<br>**DHS RCF** 5-7<br>**ICAO 9849** 1.5<br>**IEC 61850-90-12** 5.8<br>**IEEE 2030.101** 4.12-4.14 |

| **Protect**<br>**Information Protection Processes and Procedures** | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
| | well as the eventual restoration of the PNT devices and components.<br>As part of response planning, verify that systems have capabilities to mitigate PNT disruptions, such as anomaly detection with holdover capabilities. If complementary PNT sources are used, consider common failure modes and whether vulnerabilities of alternate and complementary sources are understood.<br>Response planning should consider appropriate restrictions on the downstream consumption of PNT information to limit the impact of PNT disruptions.<br>Define the incident types, resources, and management support needed to effectively maintain and mature the incident response and contingency capabilities. For critical applications and where practical, identify all known PNT system and component fault and failure modes within the deployed environments with the objective of increasing the probability that at least one PNT source will not be susceptible to each failure mode identified. For each failure and fault mode, identify detection and compensation strategies, effects on the computed PNT data, and effects on the applications dependent on the data to determine whether the response and recovery plans are adequate to meet business continuity objectives. | **ISO / IEC / IEEE 15939:2017** 6<br>**ITU-T 8262** 11<br>**IMO 1575** E.4<br>**ITU-T 8275** 7.2<br>**NIST JRES** 120.017<br>**NIST SP 800-53 Rev. 5** CP-1, CP-2, CP-7, CP-10, CP-12, CP13, IR-1, IR-7, IR-8, IR-9, PE-17<br>**NIST SP 800-160 Rev.1** Appendix F.2.6<br>**RTCA 356** 5.6.6<br>**USG FRP** 1.7.3, 6 |

| **Protect**<br>**Information Protection Processes and Procedures** | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
| | Implement mitigation strategies to temporary PNT disruptions and manipulations for all critical services. A means to maintain business continuity is leveraging complementary and holdover PNT sources and redundant components, such as antennas spaced sufficiently apart and high-stability oscillators. Select, use, and ensemble PNT sources based on system priority classifications to meet business continuity objectives. Identify complementary PNT sources with multiple phenomenologies and an understanding of the benefits, limitations, and dissimilar failure modes to increase the probability that the PNT service's ability to detect anomalous inputs and remain available in contested environments.<br><br>For responses to PNT data-dependent critical functions that involve failures or shutdowns, define and execute fail-secure or fail-safe plans for PNT systems and components. Perform PNT system acceptance testing to verify and validate response and recovery plans. For example, for systems with redundant or complementary time sources, validate current system time delivered via a time distribution protocol by removing the primary time source and confirming that the time accuracy and precision, as well as any phase or frequency steps or ramps, are in accordance with predefined clock requirements for the time server and downstream applications.<br><br>Consider the creation and maintenance of | |

| **Protect**<br>**Information Protection Processes and Procedures**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | developmental and operational test and evaluation methods to assess, verify, and validate PNT service performance under normal and contested conditions. | |
| **IP-10:**<br><br>**Response and recovery plans are tested.** | Assess threat preparedness by verifying incident response and recovery plans of the PNT systems.<br><br>For critical applications, consider qualification and periodic testing to assess PNT response and recovery plans for infrequent events (e.g., leap seconds) or changes to the components or operations that would significantly impact the performance for the system. Review the results to determine the efficiency and effectiveness of the plans as well as readiness to execute the plans. Use the results of the tests to inform other CSF functions, such as "Detect." Exercise the response and recovery plans to validate that the effects of the anomalous events on the PNT data's availability, integrity, and continuity are within specified tolerances. For example, for systems with redundant or complementary time sources, validate current system time delivered via a time distribution protocol by removing the primary time source and confirming that the time accuracy and precision, as well as any phase or frequency steps or ramps, are in accordance with pre-defined clock requirements for the time server and downstream applications.<br>Testing response and recovery plans may include the use of RF signals to simulate anomalous events. Any simulation that involves RF transmissions must be done | **DHS RCF** 8<br>**DHS S&T**<br>**ICAO 9849** 5.3.2.2<br>**IEC 61850-90-4** 14.2.4<br>**IEEE 2030.101** 5.4.2.5<br>**ITU-T GNSS** Appendix VII.3, VII.4<br>**NERC GridEx**<br>**NIST SP 800-53 Rev. 5** CP-4, IR-3, PM-14<br>**RTCA 229** 2<br>**RTCA 326** 3.4.2, 3.4.4 |

| Protect<br>Information Protection Processes and Procedures | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
| | in in a manner that is consistent with industry best practices and in accordance with laws and regulations. | |

### 4.2.5 Maintenance Category

Maintenance and repairs to industrial control and information system components are performed consistent with policies and procedures. In the context of this PNT Profile, the systems and components of interest include GNSS receivers, antennas, modules, and time servers.

Both subcategories within the Maintenance category apply to the PNT Profile, as summarized in the table below.

586 **Table 12 - Maintenance Subcategories Applicable to PNT**

| Protect<br>Maintenance<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| **MA-1:**<br><br>**Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.** | Schedule, perform, record, and review records of maintenance and repairs on PNT devices and components.<br><br>Assess the impacts of the maintenance and repair of the PNT devices and components on the end user's operations and verify that the PNT devices and components perform within specified tolerances.<br><br>Infrequent events, such as leap seconds, may be handled differently by different sources of PNT. Understand how these events and their implementations impact operations.<br><br>Make available and adhere to documentation and artifacts, such as software maintenance procedures, configuration parameters (including default values and ranges), test plans, compliance test result documentation, and other pertinent information to verify consistent and valid deployments.<br><br>Document PNT system and component calibration procedures and results for applications that require legal traceability or known uncertainty. The frequency of calibrations is dependent on factors such as environmental conditions, changes in PNT systems, components and architecture, exposure to disruptions and manipulations, and PNT data performance requirements.<br>Calibration procedures may include the absolute or relative calibration or recalibration of components. Document procedures for minimum periodic | **DHS CISA** 4<br>**DHS GPS CI**<br>**DHS RCF** 8<br>**DHS TFS** 1.6, 2, 3.6, 3.8<br>**IEEE 1139**<br>**IEEE 1193**<br>**IEEE 1588** Annex N<br>**IEEE 2030.101** 4.7, 6<br>**IETF 8633** 3.1<br>**ISO/IEC 17025**<br>**ITU-T GNSS** 2<br>**Levine 2021**<br>**NIST SP** 250-29<br>**NIST SP 800-53 Rev. 5** MA-1, MA-2, MA-3, MA-5, MA-6<br>**NIST SP 1065**<br>5-10 |

| | | |
|---|---|---|
| | calibrations to a standard reference, particularly for applications that require traceability. For example, in the U.S., legal or metrological time calibration requires an unbroken chain of documented calibrations to UTC(NIST) or UTC(USNO).<br><br>Delay variations and the stability of each component due to factors such as temperature or aging should be characterized in the environment in which the PNT system will be deployed. The calibration of component delays (e.g., antenna, surge suppressors, cables, connectors, splitters, receivers, switches) should be recorded to verify that the absolute accuracy and precision in the end-to-end systems that form and use PNT data are within specified tolerances. | |
| **MA-2:**<br><br>**Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.** | Enforce approval requirements, control, and monitoring of remote maintenance activities.<br><br>Employ the appropriate level of authentication, least privilege, logging, record keeping, and session termination for remote maintenance. | **DHS CISA** 4.b<br><br>**DHS GPS CI**<br><br>**IEEE 1588** Annex P.2.5.2<br><br>**IEEE 2030.101** 4.8.2, 4.15.2, 4.15.3, Annex G.2.4<br><br>**IETF 8633** 3.5, A.3<br><br>**NIST SP 800-53 Rev. 5** MA-4<br><br>**NIST SP 800-160 Rev. 1** Appendix F.1.14 |

### 4.2.6 Protective Technology Category

Technical security solutions are managed to verify the security and resilience of systems and assets consistent with related policies, procedures, and agreements.

There are five subcategories within the Protective Technology category that apply to the PNT Profile, as summarized in

591 the table below.

592 **Table 13 - Protective Technology Subcategories Applicable to PNT**

| Protect<br>Protective Technology<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| **PT-1:**<br><br>**Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.** | Generate audit records that contain information such as what, when, the source, the outcome, and the identity of any individuals or PNT components associated with the event. Consider maintaining audit logs for extended periods to support forensic analysis.<br><br>A log file should also include entries of proper working states in addition to entries of anomalies and events.<br><br>Wherever practical, logging and audit mechanisms should produce data elements in accordance with standard data formats to facilitate parsing and consumption by analytic teams.<br><br>PNT-dependent applications that require an audit trail often require legal or metrological traceability meaning an unbroken documented chain of calibrationsfrom a standard or other trusted reference.<br><br>As part of characterizing the physical device using or forming PNT data, determine the delay characteristics between the device clock and the time stamping functions used for the audit and logs. | **DHS CISA** 7.a<br><br>**DHS GPS CI**<br><br>**DOT 12464**<br><br>**IEEE 1588** 16.14.4.4.2<br><br>**Matsakis 2018** III, IV, V<br><br>**NIST SP 800-53 Rev. 5** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16<br><br>**NIST SP 800-160 Rev. 1** 3.3.2, 3.3.5<br><br>**SEC 613** |

| Protect<br><br>Protective Technology<br><br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| **PT-2:**<br><br>**Removable media is protected and its use restricted according to policy.** | Employ safeguards to restrict the use of portable media when used on PNT devices and components.<br><br>Ensure that PNT devices and equipment follow organizational policy on removable media. | **NIST SP 800-53 Rev. 5** MP-1, MP-2, MP-3, MP-4, MP5, MP-7, MP-8 |
| **PT-3:**<br><br>**The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.** | PNT deployment should employ the principle of least functionality.<br><br>Configure the PNT system to provide only essential capabilities.<br>When PNT data or services do not require functionality from intermediary nodes, they can be disabled to minimize attack surfaces. | **IEEE 1588** Annex P2.5.1,2.5.5<br><br>**IETF CMP** 6<br><br>**IETF 7384** 7.3<br><br>**NIST SP 800-53 Rev. 5** AC-3, CM-7 |
| **PT-4:**<br><br>**Communications and control networks are protected.** | Typically, PNT systems have high availability and integrity requirements. Identify communications and control network requirements for availability, integrity, authentication, stability, confidentiality, and other pertinent parameters based on classes of applications, and provide appropriate levels of protection.<br><br>Observe cyber hygiene in communications and control networks.<br><br>Consider appropriate measures for networks that distribute PNT data.<br><br>Some measures need to be considered at the architectural phase of the SDLC, such as transport security | **DHS CISA** 4.a, 5.a<br><br>**DHS GPS CI**<br><br>**IEEE 1588** 16.14.4.4.2, Annex P<br><br>**IETF 8633** 4.4, 5.5, 5.6<br><br>**IETF NTS** 3<br><br>**ITU-T G.8275** 8<br><br>**NIST SP 800-53 Rev. 5** AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47 |

| Protect<br>Protective Technology<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| | implementations, while others can be applied at the configuration or deployment phase, such as transport security. For example, some NTP/PTP devices have multiple network ports that could be configured to isolate control traffic.<br>As needed, consider transport security for networks that distribute PNT data. Note that implementing some transport security measures (e.g., use of cryptographic algorithms and implementations) can lead to time synchronization performance degradation that may be problematic, especially for high-precision timing applications. Verify that protective measures will not adversely affect the overall system performance requirements. | **NIST SP 800-160 Rev. 1** Appendix F |
| **PT-5:**<br>**Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.** | Mechanisms include proactive measures that reject bad PNT signals and data to limit how far threats penetrate into PNT systems. Reactive measures should also be present to handle threats that penetrate into PNT systems, including holdover capabilities paired with anomaly detection, features to limit performance degradation, and recovery capabilities.<br>Resiliency measures can also be achieved through new system designs that limit exposure times to attack surfaces, protect internal states, and have intelligent control algorithms. Some mechanisms to consider in the design phase include leveraging PNT service providers with | **DHS RCF** 5-7<br>**IEEE 1588** 9.3, 16.4, 17<br>**NIST SP 800-53 Rev. 5** CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6<br>**USG FRP** 5.1 |

| Protect<br>Protective Technology<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| | hardened signals, redundant PNT sources, fused PNT sources, or others in accordance with the resiliency requirements of the mission. | |

## 4.3 Detect Function

The Detect function addresses the development and deployment of appropriate activities to monitor for anomalous events and notify downstream users and applications upon their occurrence. The Detect function is informed by the Identify function and is enabled by the Protect function.

The objectives of the Detect function include:

- Enabling detection through monitoring and consistency checking; and
- Establishing a process for deploying and handling detected anomalies and events.

The Detect function defines three categories, all of which have subcategories that apply to the PNT Profile to varying degrees, as summarized in Sections 4.3.1 through 4.3.3.

### 4.3.1 Anomalies and Events Category

Anomalous activity is detected, and the potential impact of events is understood. In the context of this PNT Profile, this includes detection of uncharacteristic PNT data or a loss of PNT data for some period.

There are five subcategories within Anomalies and Events that apply to the PNT Profile, as summarized in the table below.

**Table 14 - Anomalies and Events Subcategories Applicable to PNT**

| **Detect**<br><br>**Anomalies and Events**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **AE-1:**<br><br>**A baseline of network operations and expected data flows for users and systems is established and managed.** | Verify that operational PNT data performance baselines and expected data flows for relevant external PNT information systems, the organization's PNT system, and applications dependent on PNT data are captured, developed, and maintained to detect events.<br><br>When practical, comply with standards-based solutions for data formatting, message formatting, and message transmission to facilitate interoperability and integration. | **DHS CISA** 1.d<br><br>**GPS ICD-870** 3.1<br><br>**IEEE 1588** Annex J<br><br>**IETF CMP**<br><br>**IMO 1575** D, D.1, D.2<br><br>**NIST SP 800-53 Rev. 5** AC-4, CA-3, CM-2, SC-16, SI-4<br><br>**RTCA 229** 1.5.2, 1.7.2<br><br>**USG FRP** Appendix B |

| | | |
|---|---|---|
| **AE-2:**<br><br>**Detected events are analyzed to understand attack targets and methods.** | Review and analyze detected events within the PNT system in (i) real time to maintain normalcy of operations; and (ii) forensically to understand the characteristics (e.g., source, data error statistics, duration, frequency, and location) of anomalous events. Be able to identify potential cyber incidents and understand attack targets and methods.<br><br>Be able to distinguish between potentially harmful events and normal operations. Be able to predict harm based on events.<br><br>Consider the PNT system when analyzing cybersecurity events involving downstream applications.<br><br>For RFI, include environmental monitoring with direction-finding capabilities to locate the source.<br><br>Preserve the raw data, analysis, and characterization to aid in the analysis of future events. | **DHS GPS CI**<br><br>**DHS RCF** 5.2<br><br>**Kaplan 2017** Chapters 9, 10<br><br>**NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, RA-5, SI-4<br><br>**RTCA 229** Appendix R<br><br>**RTCA 235** 2.1 |
| **AE-3:**<br><br>**Event data are collected and correlated from multiple sources and sensors.** | Multiple sensors and sources can be used to correlate fault modes and contribute to anomaly detection models and algorithms.<br><br>PNT data from multiple sources may be used, cross-checked, and compared for the detection of anomalous behavior.<br><br>Compile sufficient event data across the PNT system using various sources, such as event reports, logs, audit monitoring, network monitoring, physical access monitoring, environmental monitoring, and user and administrator reports.<br><br>Standards-based data formatting and serialization promotes the communication interoperability and interchangeability | **DOT CGSIC**<br><br>**GPS ICD-870** 3.1<br><br>**ICAO 9849** 5.3.3.5, 7.11<br><br>**IEEE 1588** Annex J<br><br>**IEEE 2030.101** 4.7, 4.8, 4.13, 5.4.4<br><br>**IETF CMP**<br><br>**IMO 1575** 2, 3<br><br>**NAVCEN**<br><br>**NIST SP 800-53 Rev. 5** AU-6, CA-7, CP-2, |

| | | |
|---|---|---|
| | of PNT data and supporting data.<br><br>Consider subscribing to or enabling user community and PNT provider communications for status on PNT data and services. Use authoritative sources of PNT data products, such as informational almanacs and status information, with authentication and data integrity verification capabilities. For GPS, NAVCEN has information on almanacs, operational advisories, NANU (Notice Advisory to Navstar Users), and CGSIC (Civil GPS Service Interface Committee) bulletins. Additional sector-specific advisories may be provided by ISACs and sector-specific agencies. | IR-4, IR-5, IR-8, SI-4<br><br>**NIST SP 800-160 Rev. 1** 3.3.7<br><br>**RTCA 229** Appendix G.2, G.3<br><br>**RTCA 235** 1.1<br><br>**SPD-7**<br>**USG FRP** Appendix A<br><br>**GAL ICD**<br><br>**BDS ICD** |
| **AE-4:**<br><br>**Impact of events is determined**. | Identify the effects of anomalous events on the PNT data and applications that are dependent on the PNT data. PNT events (including infrequent events and true anomalies) can have unexpected impacts on systems and operations downstream from PNT devices and equipment. Users should understand how such events might impact operations. | **DOT 12464**<br><br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, RA-3, SI-4<br><br>**RTCA 229** Appendix R |
| **AE-5:**<br><br>**Incident alert thresholds are established.** | Established PNT incident thresholds and understanding potential impacts to the mission enables proper reporting, alerting thresholds, and the development of adequate incident alert procedures.<br><br>For critical applications, document absolute or relative PNT data error and uncertainty tolerances that serve as detection thresholds, which can be expressed as a statistical distribution within the confidence levels needed for operations. For PNT-dependent applications, consider and document the required notification or alarm communication | **GPS SPS** 2.3.4<br><br>**ICAO 9849** 7.11<br><br>**IMO 1575** 2.2.1, Appendix C<br><br>**NIST SP 800-53 Rev. 5** IR-4, IR-5, IR-8<br>**USG FRP** Appendix A |

| | | |
|---|---|---|
| | time upon nearing and exceeding thresholds.<br>Based on mission requirements, consider reviewing and revising thresholds on a routine basis. | |

### 4.3.2 Security Continuous Monitoring Category

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. In the context of this PNT Profile, the interface to the PNT service provider, the receivers that process and form the PNT data, the intermediate nodes that transport PNT services, and the end applications consuming PNT data are monitored.

There are eight subcategories within the Security Continuous Monitoring category that apply to the PNT Profile, as summarized in the table below.

**Table 15 - Security Continuous Monitoring Subcategories Applicable to PNT**

| **Detect**<br>**Security Continuous Monitoring**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **CM-1:**<br>**The network is monitored to detect potential cybersecurity events.** | Monitor the PNT source and associated information products, PNT distribution, PNT data output characteristics, and additional characteristics from applications and systems dependent on PNT data against known baseline characteristics to detect anomalies, including when PNT security measures may fail.<br>Heighten system monitoring activities when there is an indication of increased risk.<br>Use an effective mix and fusion of data from multiple, diverse PNT sources and PNT data distribution routes. | **DHS CISA** 1.d<br>**DHS RCF** 7, 8<br>**DOT 12464**<br>**ICAO 9849** 5.3.1.5-5.3.1.9, 7.8<br>**IEEE 1588** 16.11, 16.12, Annex J, P.2.4<br>**IEEE 2030.101** 4.5.2<br>**IETF CMP** |

| **Detect**<br><br>**Security Continuous Monitoring**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | Consider using fault detection and exclusion algorithms to automatically detect faults and exclude erroneous sources in the computation of data used to form or that is dependent upon PNT data. This enables redundancy and consistency checking to detect changes in propagation delays and other characteristics indicating compromises in PNT data.<br><br>Verify that the monitoring strategy is sufficiently robust to detect PNT data and other system behavior anomalies for all identified fault and failure modes. Detection thresholds can be determined from nominal and anomalous data for each fault and failure mode. Consider relevant fault parameters and acceptance bounds based on reasonable or conservative criteria for various classes of applications and users.<br>Detection models can leverage correlations between fault modes and minimum detectable limits. Analysis of the correlation engines may be able to determine if some faults can remain undetected. These findings can be used in the risk management procedures.<br><br>Consider providing a loopback reference timing signal to continuously monitor for changes in the total network and signal propagation delay.<br><br>Within a specified time, alert dependent users and applications when monitoring is unavailable or when PNT data or service is unavailable.<br><br>Software and hardware can be integrated into the PNT | **IMO 1575** C.2.2, Appendix C.1<br><br>**ITU-T GNSS** Appendix III, VI<br><br>**NIST SP 800-53 Rev. 5** AU-12, CA-7, CM3, SC-5, SC-7, SI-4<br><br>**RTCA 229** 1.7.2, 1.7.3, 2.1.1.5, 2.1.3.2.2.3, 2.1.5.2.2, 2.2.1.6, 2.2.2.6<br><br>**RTCA 235** 2.3, 2.5<br><br>**USG FRP** Appendix B |

| **Detect**<br><br>**Security Continuous Monitoring**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | system and critical infrastructure components to detect and mitigate GNSS jamming and spoofing events and preserve PNT data availability, continuity, and integrity. | |
| **CM-2:**<br><br>**The physical environment is monitored to detect potential cybersecurity events.** | Physical access to PNT devices and components is actively monitored to detect potential breaches in security. Actively monitor the physical environment to include the RF environment.<br><br>PNT devices and equipment may be in remote locations. Positively identify people who access areas that contain PNT devices. Where feasible, implement the use of access controls that are specific to personnel, such as swipe cards and personal identification numbers (PINs). | **DHS GPS CI**<br><br>**ICAO 9849** 5.3.7<br><br>**Kaplan** 10<br><br>**NIST SP 800-53 Rev. 5** CA-7, PE-6, PE-20 |
| **CM-3:**<br><br>**Personnel activity is monitored to detect potential cybersecurity events.** | Monitor personnel actions for unauthorized activity on or using PNT systems or data. The scope of the monitoring can include elements such as login attributes (e.g., time, physical location, operating system, device, credentials), electronic access control systems, physical access control systems (e.g., sign in/out sheets, logging), security status monitoring of personnel activity associated with PNT systems, detecting software use, and installation restrictions. | **NIST SP 800-53 Rev. 5** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 |
| **CM-4:**<br><br>**Malicious code is detected.** | Deploy malicious code detection mechanisms, such as behavioral anomaly detection tools, throughout the PNT systems to detect and eradicate malicious code.<br><br>Should a PNT data consumer experience an anomaly, | **DHS CISA** 4.a<br><br>**NIST SP 800-53 Rev. 5** SC-44, SI-3, SI-4, |

| **Detect**<br><br>**Security Continuous Monitoring**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | consider investigating the PNT system and associated applications as possible sources of the anomaly.<br><br>Systems that use and support PNT data should be included in the antivirus analysis.<br><br>Update malicious code protection mechanisms, such as antivirus protections, when new releases are available in accordance with the configuration management policy and procedures for the PNT systems involved. | SI-8 |
| **CM-5:**<br><br>**Unauthorized mobile code is detected.** | PNT devices and equipment contain operating systems and may be vulnerable to unauthorized mobile code introduced by other vectors. Mobile code detection mechanisms throughout the enterprise are recommended because vulnerabilities' level of access may be inherited from other applications of the mobile code. | **DHS CISA** 4.a<br><br>**NIST SP 800-53 Rev. 5** SC-18, SI-4, SC-44 |
| **CM-6:**<br><br>**External service provider activity is monitored to detect potential cybersecurity events.** | Detect deviation from PNT service providers' interface specifications, which are defined in a service-level agreement (SLA) with the service provider. This can include signal integrity, availability, continuity, and coverage.<br><br>Consider subscribing to or enabling user community and PNT provider communications for status on PNT data and services. For example, NAVCEN has information on almanacs, Operational (OPS) Advisories, NANU (Notice Advisory to Navstar Users), | **DOT CMPS** 3<br><br>**GPS IS-200** 3<br>**GPS IS-705** 3<br>**GPS IS-800** 3<br>**ICAO 9849** 7.8, 7.11<br>**IMO 1575** 2.2, B.1, E.1<br>**NAVCEN** |

| **Detect**<br><br>**Security Continuous Monitoring**<br><br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | and CGSIC (Civil GPS Service Interface Committee) bulletins. Additional sector- specific advisories may be provided by ISACs and sector-specific agencies. | **NIST SP 800-53 Rev. 5** CA-7, PS-7, SA-4, SA-9, SI-4<br>**USG FRP** Appendix B |
| **CM-7:**<br><br>**Monitoring for unauthorized personnel, connections, devices, and software is performed.** | Conduct ongoing security status monitoring on PNT systems for unauthorized personnel, connections, devices, access points, and software.<br><br>Monitor for system inventory discrepancies.<br><br>Collect, aggregate, and analyze data from systems that use and support the generation and dissemination of PNT data to indicate potential unauthorized access or activity. | **NIST SP 800-53 Rev. 5** AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4<br><br>**NTP MON** |
| **CM-8:**<br><br>**Vulnerability scans are performed.** | Conduct vulnerability scans on PNT systems where safe, feasible, and in a manner that is consistent with industry best practices. Include analysis, remediation, and information sharing in the vulnerability scanning process. Ensure that scanning activities do not negatively impact online PNT devices and equipment operation. Vulnerability scanning may include the use of RF signals to simulate events such as jamming and spoofing. Any simulation that involves RF transmissions must be done in a responsible manner, according to manufacturer instructions, and in accordance with laws and regulations to avoid impacts on operations or to others.<br><br>Monitor the PNT source, network distribution characteristics | **DHS CISA** 1.a<br><br>**IEEE 2030.101** 5<br><br>**NIST SP 800-53 Rev. 5** RA-5<br><br>**NIST SP 800-115**<br><br>**RTCA 229** 1.6.2, 1.7.2, 2.1.1.1.5, 2.4, 2.5<br><br>**RTCA 326** 3.4.4<br><br>**Teasley 1995** |

| Detect<br><br>Security Continuous Monitoring | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
| | (e.g., delays, jitter, bandwidth saturation), signal distribution medium characteristics (e.g., timing delays), PNT data output, and additional characteristics from applications and systems that are dependent on PNT data for anomalous behavior, including when security measures may fail and the system needs to fail-secure or fail-safe.<br><br>All sources of PNT, including alternate or complementary PNT devices, need to be tested and enabled in advance of a PNT disruption event. | |

### 4.3.3 Detection Processes Category

Detection processes and procedures are maintained and tested to promote awareness of anomalous events. In the context of this PNT Profile, the process and procedures on the information systems and assets as well as the analytic processes and procedures are maintained, updated, and tested.

There are four subcategories within the Detection Process category that apply to the PNT Profile, as summarized in the table below.

**Table 16 - Detection Processes Applicable to PNT**

| Detect<br><br>Detection Processes | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |

| | | |
|---|---|---|
| **DP-1:**<br><br>**Roles and responsibilities for detection are well-defined to ensure accountability.** | When feasible, provision roles and responsibilities within a cooperative detection framework for data collection, data storage, and data dissemination towards improving future PNT protection, detection, response, and recovery capabilities.<br><br>Understand PNT service provider and sector specific PNT detection roles and responsibilities. | **DHS IDM**<br>**DOT CMPS** 1.3<br>**ICAO 9849** 7.8<br>**NIST SP 800-53 Rev. 5** CA-2, CA-7, PM-14<br>**USG FRP** 2.1-2.4, 3.2.11 |
| **DP-3:**<br><br>**Detection processes are tested.** | Validate that event detection processes are operating as intended. PNT devices and components that are upgraded are re-validated with end-to-end testing by the users.<br>Perform periodic testing to verify the performance of the detection process against the most current threat profiles and vulnerabilities. | **DHS RCF** 6<br>**DHS S&T**<br>**NIST SP 800-53 Rev. 5** CA-2, CA-7. PM-14, SI-3, SI-4<br>**RTCA 229** 1.7.2, 1.7.3, 1.8.2.3, 2.1.1.4.1, 2.1.1.5, 2.1.1.13, 2.1.2.2, 2.1.3.2, 2.1.4.2, 2.1.4.9, 2.1.5.2, 2.4.1.1, 2.5.3, 2.5.7, 2.5.9-2.5.11<br>**RTCA 326** 3.4.4 |
| **DP-4:**<br><br>**Event detection information is communicated.** | Communicate PNT data anomaly detection and the current best estimate of PNT data quality to personnel, partners, analytics, and downstream application users.<br>When the cause of a PNT service disruption event is suspected to be external, share event detection with the appropriate external stakeholders for further investigation. | **ICAO 9849** 7.12, Appendix F<br>**IEEE 1588** 7.6.2, 16.11, 16.12<br>**IEEE C37.238** 6.2.1, 6.3<br>**IETF CMP**<br>**IMO 1575** 2.3, B.2.2.1<br>**ITU-T G.8275** Appendix II, IV<br>**NIST SP 800-53 Rev. 5** AU-6, CA-2, CA-7, RA5, SI-4<br>**RTCA 229** 2.1.1.4 |

| | | |
|---|---|---|
| | | **USG FRP** Appendix B |
| **DP-5:**<br><br>**Detection processes are continuously improved.** | Modify and improve the monitoring strategy as new fault modes are identified and until detection performance is acceptable.<br><br>Periodically examine the organization's PNT anomaly detection processes and seek to improve them continuously. | **NIST SP 800-53 Rev. 5** CA-2, CA-5, CA-7, PL-2, PM-14, RA-5, SI-4 |

## 4.4 Respond Function

Develop and implement the appropriate activities to respond to a detected cybersecurity or anomalous event. The activities in the Respond Function function support the ability to contain the impacts of a disruption or manipulation to PNT services or data.

The Respond Function function serves as a list of recommended actions and is triggered by the outputs generated by the Detect Functionfunction. The Protect Function function provides the ability for the Respond Function function to execute the proper response to an event according to a predefined plan.

The objectives of the Response function are to:

- Contain PNT events using a verified response procedure
- Communicate the occurrence and impact of the event on PNT data to PNT data users, applications, and stakeholders
- Develop processes to respond to and mitigate new known or anticipated threats or vulnerabilities; and
- Evolve response strategies and plans based on lessons learned

The Respond function within the Cybersecurity Framework defines five categories, all of which have at least one subcategory that applies to the PNT Profile to varying degrees, as summarized in Sections 4.4.1 through 4.4.5.

### 4.4.1 Response Planning Category

Response processes and procedures are executed and maintained after detected cybersecurity incidents.

There is one subcategory within Response Planning that applies to the PNT Profile, as summarized in the table below.

**Table 17 - Response Planning Subcategory Applicable to PNT**

| **Respond**<br>**Response Planning**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **RP-1:**<br>**Response plan is executed during or after an incident.** | Execute the response plan during or after a cybersecurity event that affects PNT systems in accordance with the predefined threshold.<br>Document the steps and results of the response plans as they are being executed. Include categories of incidents and PNT resilience level requirements based on application criticality and impact.<br>Update the response plans to address changes to the organization, such as PNT system, attack vectors, environment of operation, and problems encountered during plan implementation, execution, and testing. | **DHS RCF** 5.3, 5.4, 6<br>**IMO 1575** C.2.1, C.2.2<br>**NIST SP 800-53 Rev. 5** CP-2, CP-10, IR-4, IR-8 |

### 4.4.2 Communications Category

Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies). In the context of this PNT Profile, external stakeholders may include sources that announce events that will impact the PNT service, such as PNT interference or corrections for leap seconds.

643 There are four subcategories within the Communications category that apply to the PNT Profile, as summarized in the table below.

644 **Table 18 - Communications Subcategories Applicable to PNT**

| **Respond**<br>**Communications** | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
| **CO-1:**<br>**Personnel know their roles and order of operations when a response is needed.** | Verify that personnel are trained to respond to PNT disruptions and manipulations and understand recovery time objectives (RTO), recovery point objectives (RPO), restoration priorities, task sequences, and assignment responsibilities for event response programs and processes in a manner that is consistent with business continuity objectives. | **DHS CISA** 1.f, 7.a<br>**DHS RCF** 5.2, 8.3<br>**IMO 1575** C.2.2<br>**NIST SP 800-61**<br>**NIST SP 800-34 Rev.1** 3.2.1, CP-2, CP-3, IR-3, IR-8<br>**NIST SP 800-53 Rev. 5** CP-2, CP-3, IR-3, IR-8<br>**USG FRP** 5.1.2.5 |
| **CO-2:**<br>**Incidents are reported consistent with established criteria.** | Verify that cybersecurity events on the PNT system are reported in a manner consistent with the response plan.<br><br>Suspected intentional interference should be reported to stakeholders through the appropriate channels and procedures. For example, suspected land-based RFI can be reported to NAVCEN, NASA Aviation Safety Reporting System for aeronautics, or NERC E-ISAC for the electric utility sector. | **DHS IDM**<br>**ICAO 9849** 7.12, Appendix F 6.1.1<br>**NAVCEN**<br>**NIST SP 800-53 Rev. 5** AU-6, IR-6, IR-8<br>**NIST SP 800-61 Rev. 2** 4 |

| **Respond**<br>**Communications**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | | **NERC CIP-008-6**<br>**NERC EISAC**<br>**USG FRP** |
| **CO-3:**<br>**Information is shared consistent with response plans.** | Share cybersecurity incident information with relevant stakeholders as defined in the organizational sharing policies.<br>Where feasible, consider enabling PNT systems and PNT data information sharing to alert downstream users and applications of a disruption or manipulation of PNT data, allowing applications and users to respond in near real-time based on application tolerances. | **DHS CISA** 1.d, 1.f<br>**DHS IDM**<br>**FCC**<br>**ICAO 9849** 7.12, Appendix F 6.1.1<br>**IEEE 1588** 7.6.2, 16.11, 16.12<br>**IETF CMP**<br>**NAVCEN**<br>**NERC EISAC**<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8<br>**NIST SP 800-61 Rev. 2** 2.4 |
| **CO-4:**<br>**Coordination with stakeholders occurs consistent with response plans.** | In the event of PNT disruption or manipulation, coordinate PNT cybersecurity incident response actions with all relevant stakeholders in accordance with predefined agreements.<br>When agreed upon between stakeholders, common data formats facilitate information sharing to strengthen the protection of the user community. | **DHS IDM**<br>**NERC EISAC**<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8, PE-6<br>**NIST SP 800-61 Rev. 2** 2.4 |

### 4.4.3 Analysis Category

Analysis is conducted to verify effective response and support recovery activities. In the context of this PNT Profile, the analysis will include the direct recipients of PNT services as well as secondary or downstream effects.

There are five subcategories within the Analysis category that apply to the PNT Profile, as summarized in the table below.

**Table 19 - Subcategories Applicable to PNT**

| **Respond**<br>**Analysis**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **AN-1:**<br>**Notifications from detection systems are investigated.** | Investigate cybersecurity-related notifications generated from PNT anomaly detection systems.<br>Identify and locate potential sources of RFI.<br>After determining that the source of a PNT data anomaly is external to the organization's system, partner with the appropriate external stakeholders for further investigation. DHS coordinates development, implementation, and exercise of procedures to enable federal agencies with assigned responsibilities, authorities, and jurisdictions to investigate and mitigate GNSS-based PNT interference.<br>Should multiple sensors report data anomaly events, analytics can be used to determine if the events are correlated or otherwise traced to a common causal agent. | **DHS IDM**<br>**ICAO 9849** Appendix F 6.2<br>**NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, PE-6, RA-5, SI-4<br>**RTCA 235** 14.1.2 |
| **AN-2:**<br>**The impact of the incident** | Understand the full implication of a cybersecurity incident based on thorough investigation and analysis | **ITU-T G.8275.1** Annex D |

| **Respond**<br>**Analysis**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **is understood.** | results.<br>Consider the organizational impacts on PNT services that may affect downstream applications, users, and systems that are dependent on PNT.<br>Understand downstream impacts and relationships through leveraging mapped services and outlined policies.<br>Understand the scope and necessary actions required for remediation. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, RA-3<br>**NIST SP 800-61 Rev. 2** 3 |
| **AN-3:**<br>**Forensics are performed.** | Conduct forensic analysis on collected cybersecurity event information to determine if the adversary left a footprint or if there are any residual effects to the system.<br>Conduct forensic analysis to aid in determination of the root cause of PNT disruption or manipulation. | **ICAO 9849** Appendix F 6.2<br>**NIST SP 800-53 Rev. 5** AU-7, IR-4<br>**NIST SP 800-61 Rev. 2** 3 |
| **AN-4:**<br>**Incidents are categorized consistent with response plans.** | Categorize cybersecurity incidents according to the level of severity and impact consistent with the response plan. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-5, IR-8, RA-3<br>**NIST SP 800-61 Rev. 2** 2 3.2 |
| **AN-5:**<br>**Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization** | For PNT components and applications that are dependent on PNT data, identify verification and validation procedures and processes for anticipated and known threats in response to existing and newly identified PNT fault and failure modes, including interfering signals, natural phenomena, and internal system failures. | **DHS RCF** 7, 8<br>**DOT 12464**<br>**GPS-ICD-240**<br>**ICAO 9849** 7.6, 7.7 |

| Respond<br>Analysis<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| **from internal and external sources (e.g., internal testing, security bulletins, or security researchers).** | Reference available public and private trusted sources of threat and vulnerability intelligence information as it relates to PNT.<br>Update PNT disruption event characterization documentation as well as organization or industry-shared databases to track the observed probability of occurrence in order to continuously update the risk assessment and response plans. Analyze the impact of the PNT data anomaly on user and application errors. Characterize nominal and anomalous PNT data from the incident for improving future monitoring and detection. | **NCCIC**<br>**NIST SP 800-53 Rev. 5** CA-1, CA-2, PM-4, PM-15, RA-1, RA-7, SI-5, SR-6<br>**NIST SP 800-61 Rev. 2** 3, 3.2<br>**NIST SP 800-160 Rev. 1** 3.4.9, 3.4.11<br>**NTP SEC**<br>**RTCA 326** 3.4.4<br>**RTCA 356** 3.8<br>**USG FRP** Appendix B |

### 4.4.4 Mitigation Category

Activities are performed to contain an event, mitigate its effects, and resolve the incident. In the context of PNT, mitigation measures may include failover to alternate or a fusion of PNT sources, notification to or from external stakeholders of ongoing PNT anomalies, and other activities.

There are three subcategories within the Mitigation Category that apply to the PNT Profile, as summarized in the table below.

655 **Table 20 - Mitigation Subcategories Applicable to PNT**

| **Respond**<br>**Mitigation**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **MI-1:**<br>**Incidents are contained.** | Contain cybersecurity incidents to minimize impacts on the PNT system.<br>Containment of a PNT event may require notification of downstream users and the transition to alternate or complementary PNT sources in accordance with resiliency level requirements and the business continuity plan for containment. | **DHS GPS CI**<br>**NIST SP 800-53 Rev. 5** IR-4<br>**NIST SP 800-61 Rev. 2** 3.4.1 |
| **MI-2:**<br>**Incidents are mitigated.** | Given successful containment measures, implement PNT-based mitigation measures that can include alternate or complementary sources in order to operate through the incident.<br>Once the effects of the incident are contained, take steps to return the PNT system to a proper working state. These steps may include resetting, recalibration, and replacement of units in a manner that does not impact forensic efforts.<br>Apply patches and updates to mitigate the vulnerability or incident.<br>Mitigation procedures or measures should be part of the business continuity plan.<br>Consider mitigation strategies such as PNT source and data path redundancy, diversity, and segmentation to minimize the impacts of PNT disruption or manipulation. | **3GPP TR22.878** 4, 5<br>**DHS GPS CI**<br>**DHS RCF** 5.3, 5.4<br>**IMO 1575** C.2.1, C.2.2<br>**ITU-T G.8262** 11<br>**ITU-T G.8272** 7<br>**Kaplan** 1.8, 13<br>**NIST SP 800-53 Rev. 5** IR-4<br>**NIST SP 800-61 Rev. 2** 3.4<br>**NTP SEC**<br>**USG FRP** 4 |

| **Respond**<br>**Mitigation**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| | Complementary or alternative PNT sources may include on-board sensors, clocks with acceptable holdover characteristics, other satellite constellations, signal frequencies, terrestrial RF sources (e.g., cellular, TBS), network-based PNT sources (e.g., NTP, PTP), and other signals of opportunity. | |
| **MI-3:**<br>**Newly identified vulnerabilities are mitigated or documented as accepted risks.** | Risk assessments (refer to RA-1) should be updated with newly identified PNT vulnerabilities and mitigated or documented as acceptable risks.<br>Maintain an RFI incident database in order to inform future mitigation strategies. | **NIST SP 800-53 Rev. 5** CA-2, CA-7, RA-3, RA-5, RA-5<br>**NIST SP 800-61 Rev. 2** 3<br>**NTP SEC**<br>**RTCA 235** 14.1.4, 14.2-14.4<br>**RTCA 356** 3.8 |

### 4.4.5 Improvements Category

Organizational response activities are improved by incorporating lessons learned from current and previous detection and response activities. Both subcategories within the Improvements category apply to the PNT Profile, as summarized in the table below.

**Table 21 - Improvements Subcategories Applicable to PNT**

| **Respond**<br>**Improvements** | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
| **IM-1:**<br><br>**Response plans incorporate lessons learned.** | PNT response plans incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing and implement the resulting changes accordingly. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8<br><br>**NIST SP-800-61 Rev. 2** |

| Respond<br>Improvements | | |
|---|---|---|
| **Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
| **IM-2:**<br><br>**Response strategies are updated.** | Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned.<br><br>Analyze detected event information and incident responses to gain perspective on the impacts to the organization. Then correlate with and, if necessary, update the risk assessment.<br><br>Determine preventative actions for fault modes by reviewing the identification, protection, and detection functions and updating as applicable.<br><br>Revise protection, monitoring, detection, response, and recovery capabilities as needed to mitigate newly identified vulnerabilities in a timely manner.<br><br>Industry standards may also need to evolve with new PNT capabilities, taking into account changes in threat models as well as technical, operational, and economic factors. | **DHS IDM**<br><br>**DOT 12464**<br><br>**ICAO 9849** 6.3, 6.4, 6.5, 6.7, 6.8, 6.9<br><br>**IMO 1575** E.1<br><br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8<br><br>**NTP SEC**<br><br>**RTCA 326** 3.4.1 |

## 4.5 Recover Function

The Recover function develops and implements 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 and return the organization back to its proper working state after a disruption or manipulation of PNT services has occurred. The effectiveness of the Recover function is dependent upon implementation of the previous functions—Identify, Protect, Detect, and Respond.

667 The objectives of the Recovery function are to:

668 • Restore systems dependent upon PNT services to a proper working state using a verified recovery procedure;
669 • Communicate recovery activities and status of the PNT services to PNT data users, applications, and stakeholders; and
670 • Evolve recovery strategies and plans based on lessons learned.

671 The Recover function within the NIST Cybersecurity Framework defines three categories. Other than identify appropriate
672 PNT sources, all these categories and subcategories correlate with all the components of the EO.

### 4.5.1 Recovery Planning Category

Recovery processes and procedures are executed and maintained to restore systems or assets affected by cybersecurity incidents to a proper working state.

There is one subcategory within Recovery Planning that applies to the PNT Profile.

**Table 22 - Recovery Planning Subcategory Applicable to PNT**

| **Recover**<br>**Recovery Planning**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **RP-1:**<br>**Recovery plan is executed during or after a cybersecurity incident.** | The business continuity plan should include a recovery plan. Execute the recovery plan during or after a cybersecurity incident on the PNT system.<br>Restore the PNT system within a predefined, acceptable time period from configuration-controlled and integrity-protected information representing a known, operational state for the components.<br>The recovery capability of the equipment, including devices that can operate through an incident, is part of a PNT system's recovery process. Perform system acceptance testing.<br>The recovery plan can include specific actions for restoration, recalibration, resetting, and test validation of equipment. | **DHS RCF** 5, 6<br>**ICAO 9849** 7.7<br>**IEEE 2030.101** 5<br>**NIST SP 800-34 Rev. 1**<br>**NIST SP 800-53 Rev. 5** CP-10, IR-4, IR-8<br>**NIST SP 800-160 Rev. 1** 3.4.11, Appendix F.2.6<br>**NIST SP 800-184**<br>**RTCA 229** 2.4, 2.5 |

### 4.5.2 Improvements Category

Recovery planning and processes are improved by incorporating lessons learned into future activities. In the context of this PNT Profile, the efficacy of the recovery actions, such as restoration of the PNT system, test plans, user notification and failover, are evaluated and improved should a similar event occur.

There are two subcategories within the Improvements category that apply to the PNT Profile, as summarized in the table below.

**Table 23 - Improvements Subcategories Applicable to PNT**

| **Recover**<br>**Improvements**<br>**Subcategory** | **Applicability to PNT** | **References (PNT-Specific)** |
|---|---|---|
| **IM-1:**<br><br>**Recovery plans incorporate lessons learned.** | PNT recovery plans incorporate lessons learned from ongoing incident handling activities into incident recovery procedures, training, and testing and implement the resulting changes accordingly.<br><br>Update the vulnerability, threat, impact, and risk assessment. The data and resulting analysis will assist in the analyses of future events, updating risk assessments, and the development of monitoring, detection, response, and recovery features. | **DOT 12464**<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8<br>**NIST SP 800-61 Rev. 2** 3.4<br>**NTP SEC** |

| Recover<br>Improvements<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| **IM-2:**<br>**Recovery strategies are updated.** | Update the recovery plan to incorporate lessons learned, reflect new threats, improve technology, and address changes to the organization, PNT system, operating environment, and problems encountered during plan implementation, execution, and testing.<br>Recovery timeliness and prioritization based on application criticality are key to reducing impacts. Evaluate incident characteristics to determine the optimal recovery strategy and revise the recovery plan as needed. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8<br>**NIST SP 800-61 Rev. 2** 3.4<br>**RTCA 326** 3.4.1 |

### 4.5.3 Communications Category

Restoration activities are coordinated with internal and external parties. In the context of this PNT Profile, external parties may include industry associations that provide insight with respect to how PNT services are restored after a PNT event, such as RFI. Restoration activities can include corrections for anomalies, calibrations, verification, and validation procedures.

There are three subcategories within the Communications category that apply to the PNT Profile, as summarized in the table below.

689 **Table 24 - Communications Subcategories Applicable to PNT**

| Recover<br>Communications<br>Subcategory | Applicability to PNT | References (PNT-Specific) |
|---|---|---|
| **CO-1:**<br>**Public relations are managed.** | Centralize and coordinate information distribution and manage the public-facing representation of the organization.<br>Public relations management may include managing media interactions, creating privacy policies, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and email requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of the information provided to the media, and ensuring that personnel are familiar with public relations. | **NIST SP 800-34 Rev. 2** 4<br>**NIST SP 800-53 Rev. 5** IR-4<br>**NIST SP 800-184** 2.4 |
| **CO-2:**<br>**Reputation is repaired after an incident.** | Employ a crisis response strategy to protect against negative impacts and repair organizational reputation.<br>Crisis response strategies may include actions to shape attributions of the crisis, change perceptions of the organization in crisis, and reduce the negative effects generated by the crisis. | **NIST SP 800-53 Rev. 5** IR-4<br>**NIST SP 800-184** (all sections) |
| **CO-3:**<br>**Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.** | Communicate recovery activities to all relevant internal and external stakeholders, executive teams, and management teams. | **DOT 12464**<br>**DHS S&T**<br>**NIST SP 800-34 Rev. 2**<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4<br>**NIST SP 800-184**<br>**NTP SEC** |

690

# References

[3GPP TS22.071] 3rd Generation Partnership Project (2022) Location Services (LCS) Service description Stage 1(Release 17) March 2022. (Technical Specification Group Services and System Aspects, Sophia Antipolis, France). Specification 22.071. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=584

[3GPP TR22.826] 3rd Generation Partnership Project (2021) Study on Communication Services for Critical Medical Applications (Release 17.2) March 2021. (Technical Specification Group Services and System Aspects, Sophia Antipolis, France). Specification 22.826. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetail s.aspx?specificationId=3546

[3GPP TR22.878] 3rd Generation Partnership Project (2021); Feasibility Study on 5G Timing Resiliency System (Release 18.2) December 2021. (Technical Specification Group Services and System Aspects, Sophia Antipolis, France). Specification TR.878. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetail s.aspx?specificationId=3769

[3GPP TS36.305] 3rd Generation Partnership Project (2022) Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN (Release 17) (Radio Access Network Evolved Universal Terrestrial Radio Access Network (E- UTRAN,) March 2022. Specification TS36.305. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetail s.aspx?specificationId=2433

[ATIS-I-0000070] ATIS-I-0000070 (2018) *Context-Aware Identity Management Framework*. (ATIS, Washington, DC). Available at https://access.atis.org/apps/group_public/download.php/43565/ATIS-I-0000070.pdf

[Barret 2018] Barrett M (2018) *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework*. Available at: https://doi.org/10.6028/NIST.CSWP.04162018

[BDS ICD] China Satellite Navigation Office (2019) *BeiDou Navigation Satellite System Signal In Space Interface Control Document Open Service Signal B1I Version 3.0*.

[CNSSI 4009] Committee on National Security Systems (2015) *Committee on National Security Systems Glossary*. Committee on National Security Systems Instruction (CNSSI) No. 4009, April 2015. Available at

https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

[DHS CISA] Cybersecurity & Infrastructure Security Agency (2020) Time Guidance for Network Operators, Chief Information Officers, and Chief Information Security Officers. (DHS, Washington, DC). Available at https://www.cisa.gov/sites/default/files/publications/time_guidance_network_operators_cios_cisos_508.pdf

[DHS GPS CI] Department of Homeland Security. Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure. (DHS, Washington, DC). Available at https://www.cisa.gov/uscert/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf

[DHS IDM] Department of Homeland Security (2008) United States Positioning, Navigation, and Timing Interference Detection and Mitigation Plan ummary. (DHS, Washington, DC). Available at https://www.gps.gov/news/2008/2008-04-idm-public-summary.pdf

[DHS PNT] Department of Homeland Security (2020) Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS.) (DHS, Washington, DC).Available at https://www.cisa.gov/sites/default/files/publications/report- on-pnt-backup-complementary-capabilities-to-gps_508.pdf

[DHS RCF] Department of Homeland Security (2022) Resilient PNT Conformance Framework. (DHS, Washington, DC). Available at https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf

[DHS S&T] Department of Homeland Security (2020) *Science and Technology Position, Navigation, and Timing (PNT) Program.* (DHS, Washington, DC). Available at https://www.dhs.gov/science-and-technology/pnt-program

[DHS S&T 2022] Department of Homeland Security (2022) *Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture Version 1.0.* (DHS, Washington, DC). Available at https://www.dhs.gov/science-and-technology/publication/resilient-pnt-reference-architecture

[DHS TFS] Department of Homeland Security (2015) Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations. (DHS, Washington, DC). Available at https://www.dhs.gov/sites/default/files/publications/GPS-PNT-Best-Practices-Time-Frequency-Sources-Fixed-Locations-508.pdf

[DIA] Defense Intelligence Agency (2022) DIA Challenges to Security in Space. (DIA, Washington, DC). Available at https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf

[DOT] Department of Transportation. *What is Positioning, Navigation and Timing (PNT)?* (Department of Transportation, Washington, DC). Available at https://www.transportation.gov/pnt/what-positioning-navigation-and-timing-pnt

[DOT CGSIC] Department of Transportation. (2020) *Civil GPS Service Interface Committee.* (Department of Transportation. Washington, DC.) Available at https://www.gps.gov/cgsic/

[DOT CMPS] Department of Transportation (2020) *Global Positioning System (GPS) Civil Monitoring Performance Specification, 3rd Edition*. (Department of Transportation, Washington, DC), GPS Civil Monitoring Performance Specification DOT-VNTSC-FAA-20-08. Available at https://www.gps.gov/technical/ps/2020-civil-monitoring-performance-specification.pdf

[DOT 12464] Van Dyke K, Kovach K, Lavrakas J (2004) Status Update on GPS Integrity Failure Modes and Effects Analysis. (Department of Transportation, Washington, DC). Available at https://rosap.ntl.bts.gov/view/dot/12464/dot_12464_DS1.pdf

[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

[FCC] Federal Communications Commission (2020) Jammer Enforcement. (FCC, Washington DC). Available at https://www.fcc.gov/general/jammer-enforcement

[FCC E911] Federal Communications Commission (2020) Wireless E911 Location Accuracy Requirements Sixth Report and Order and Order on Reconsideration-PS Docket No. 07-114 (FCC, Washington DC). Available at https://docs.fcc.gov/public/attachments/DOC-365168A1.pdf

[FINRA 4590] Financial Industry Regulatory Authority (2016) *4590. Synchronization of Member Business Clocks.* (FINRA, Washington, DC). Available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/4590

[GAL ICD] European GNSS (Galileo) Open Service (2021) *Signal-in-Space Interface Control Document Issue 2.0.* (European Union). Available at https://www.gsc-

europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.0.pdf

[GPS] Department of Homeland Security, US Coast Guard (1996) *Navstar GPS User Equipment Introduction.* (U.S. Coast Guard Navigation Center, Department of Homeland Security, Alexandria, VA), September 1996.

[GPS ICD-240] SAIC (GPS SE&I) (2021) *Navstar GPS Control Segment to User Support Community.* (Air Force Space Command, Department of Homeland Security, and the U.S. Coast Guard, Washington, DC), Global Positioning System Interface Control Document ICD-GPS-240C. Available https://www.gps.gov/technical/icwg/ICD-GPS-240D.pdf

[GPS ICD-870] SAIC (GPS SE&I) (2020) *NAVSTAR Next Generation GPS Control Segment (OCX) to User Support Community Interface*. (Air Force Space Command, Department of Homeland Security, Department of Transportation, Federal Aviation Administration, and the U.S. Coast Guard, Washington, DC), Global Positioning System Interface Control Document ICD-GPS-870E. Available at https://www.gps.gov/technical/icwg/ICD-GPS-870E.pdf

[GPS GNSS] National Coordination Office for Space-Based Positioning, Navigation, and Timing (2020) *Other Global Navigation Satellite Systems (GNSS).* Available at https://www.gps.gov/systems/gnss/

[GPS IS-200] SAIC (GPS SE&I) (2021) *NAVSTAR GPS Space Segment/Navigation User Segment Interfaces*. (Air Force Space Command, Washington, DC) , Global Positioning System Interface Specification Document IS-GPS- 200M. Available at https://www.gps.gov/technical/icwg/IS-GPS-200M.pdf

[GPS IS-705] SAIC (GPS SE&I) (2021) *NAVSTAR GPS Space Segment/User Segment L5 Interfaces*. (Air Force Space Command, Washington, DC) , Global Positioning System Interface Specification Document IS-GPS-705D. Available at https://www.gps.gov/technical/icwg/IS-GPS-705H.pdf

[GPS IS-800] SAIC (GPS SE&I) (2021) *NAVSTAR GPS Space Segment/User Segment L1C Interfaces*. (Air Force Space Command, Washington, DC) , Global Positioning System Interface Specification Document IS-GPS-800D. Available at https://www.gps.gov/technical/icwg/IS-GPS-800H.pdf

[GPS SPS] U.S. Department of Defense (2020) *Global Positioning System (GPS) Standard Positioning Service Performance Standard*, 5th Edition. (Department of Defense, Washington, DC). Available at https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf

[ICAO 9849] International Civil Aviation Organization (2017) *Doc 9849 Global Navigation Satellite System Manual.* Third edition. (Montréal, Québec). Available at https://www.icao.int/Meetings/anconf12/Documents/Doc.%209849.pdf

[ICS-CERT] Cybersecurity & Infrastructure Security Agency (2020) Industrial Control Systems. (DHS, Washington, DC). Available at https://us-cert.cisa.gov/ics

[IEC 61850-90-4] International Electrotechnical Commission (2020) *IEC 61850-90-4: 2020 Communication Networks and Systems for Power Utility Automation - Part 90-4: Network Engineering Guidelines* (IEC, Geneva, Switzerland). Available at https://webstore.iec.ch/publication/64801

[IEC 61850-90-12] International Electrotechnical Commission (2020) *IEC 61850-90-12:2020 Communication networks and systems for power utility automation - Part 90-12: Wide area network engineering guidelines.* (IEC Geneva, Switzerland). Available at https://webstore.iec.ch/publication/63706

[IEC 62439-3] International Electrotechnical Commission (2021) *IEC 62439-3 Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).* (IEC, Geneva, Switzerland). Available at https://webstore.iec.ch/publication/64423

[IEEE C37.238] IEEE Standards Association (2017) *IEEE C37.238:2017 IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications* (IEEE SA, Piscataway, NJ). Available at https://standards.ieee.org/standard/C37_238-2017.html

[IEEE 802.1AS] IEEE Standards Association (2020) *IEEE 802.1AS Timing and Synchronization for Time Sensitive Applications* (IEEE SA, Piscataway, NJ). Available at https://standards.ieee.org/ieee/802.1AS/7121/

[IEEE 1588] IEEE Standards Association (2019) *IEEE 1588:2019 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control System* (IEEE SA, Piscataway, NJ). Available at https://standards.ieee.org/standard/1588-2019.html

[IEEE 1139] IEEE Standards Association (2008) *IEEE 1139:2008 Standard Definitions of Physical Quantities for Fundamental Frequency and Time Metrology---Random Instabilities* (IEEE SA, Piscataway, NJ). Available at doi: 10.1109/IEEESTD.2008.4797525.

[IEEE 1193] IEEE Standards Association (2003) *IEEE 1193:2003 IEEE Guide for Measurment of Environmental Sensitivities of Standard Frequency*

*Generators* (IEEE SA, Piscataway, NJ). Available at doi: 10.1109/IEEESTD.2004.94440. (*Undergoing Revision)*

[IEEE 2030.101] IEEE Standards Association (2018) *IEEE 2030.101:2018 Guide for Designing a Time Synchronization System for Power Substations* (IEEE SA, Piscataway, NJ). Available at https://standards.ieee.org/standard/2030_101-2018.html

[IETF 4082] Perrig A, Song D, Canetti D, Tygar, JD, Briscoe, B (2005) Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 4082. Available at https://tools.ietf.org/html/rfc4082

[IETF 5905] Mills, D, Martin, J, Burbank, J, and Kach, W. ,*Network Time Protocol Version 4: Protocol and Algorithms Specification.* (Internet Engineering Task Force (IETF) Network Working Group) Available at https://datatracker.ietf.org/doc/html/rfc5905

[IETF 7384] Mizrahi T (2014) Security Requirements for Time Protocols in Packet Switched Networks. Introduction (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 7384. Available at https://tools.ietf.org/html/rfc7384

[IETF 8573] Malhotra A, Goldberg S (2019) Message Authentication Code for the Network Time Protocol (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 8573. Available at https://tools.ietf.org/html/rfc8573

[IETF 8633] Reilly D, Stenn H, Sibold D (2019) Network Time Protocol Best Current Practices. (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 8633. Available at https://tools.ietf.org/html/rfc8633

[IETF 8915] Franke D, Sibold D, Danserie M, Sunblad R, Teichel K (2020) Using the Network Time Security Specification to Secure the Network Time Protocol. (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 88915. Available at https://tools.ietf.org/html/rfc8915

[IETF CMP] Haberman B (2020) Control Messages Protocol for Use with Network Time Protocol. Internet Engineering Task Force (IETF) Network Working Group), V4 Draft. Available at https://tools.ietf.org/html/draft-ietf-ntp- mode-6-cmds-10

[IETF NTS] Franke D, Sibold D, Teichel K, Dansarie M, Sundblad R (2020) Network Time Security for the Network Time Protocol Internet Engineering Task Force (IETF) Network Time Protocol Working

Group). Available at https://tools.ietf.org/html/draft-ietf-ntp-using-nts-for-ntp-28

[IMO 1575] International Maritime Organization (2017) MSC.1/Circular.1575 - Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing Guidelines for Shipborne Position, Navigation and Timing. (IMO, London, England). Available at https://www.imorules.com/MSCCIRC_1575.html

[ISO 17025] International Organization for Standardization (2017) *ISO/IEC 17025 General Requirements for the Competence of Testing and Calibration Laboratories*. (ISO, Geneva, Switzerland), Corrigendum 1, Mar. 2018. Available at https://www.iso.org/standard/66912.html

[ITU-T 810] International Telecommunications Union Telecommunications Standardization Sector (1996) *ITU-T G.810, Definitions and Terminology for Synchronization Networks.* (ITU-T, Geneva, Switzerland), Corrigendum 1, Nov. 2001. Available at https://www.itu.int/rec/T-REC-G.810/en

[ITU- T G.8261] International Telecommunications Union Telecommunications Standardization Sector (2019) *ITU-T G.8261/Y.1361 Timing and synchronization aspects in packet networks.* (ITU-T, Geneva, Switzerland). Available at https://www.itu.int/rec/T-REC-G.8261-201908-I/en

[ITU- T G.8262] International Telecommunications Union Telecommunications Standardization Sector (2018) *ITU-T G.8262/Y.1367 Timing Characteristics of Primary Reference Time Clocks.* (ITU-T, Geneva, Switzerland). Available at https://www.itu.int/rec/T-REC-G.8262

[ITU- T G.8272] International Telecommunications Union Telecommunications Standardization Sector (2018) *ITU-T G.8262/Y.1367 Timing Characteristics of Primary Reference Time Clocks.* (ITU-T, Geneva, Switzerland). Available at https://www.itu.int/rec/T-REC-G.8272/en

[ITU-T G.8275.1] International Telecommunications Union Telecommunications Standardization Sector (2022) ITU-T G.8275.1/Y.1369.1 Amendment 3 *Precision Time Protocol Telecom Profile for Phase/Time Synchronization with Full Timing Support from The Network.* (ITU-T, Geneva, Switzerland). Available at https://www.itu.int/rec/T-REC-G.8275.1/en

[ITU-T GNSS] International Telecommunications Union Telecommunications Standardization Sector (2020) *ITU-T GSTR-GNSS Considerations on the use of GNSS as a primary time reference in telecommunications* (ITU-T, Geneva, Switzerland). Available at https://www.itu.int/dms_pub/itu- t/opb/tut/T-TUT-HOME-2020-PDF-

E.pdf

[Kaplan 2017] Kaplan E, Hegarty C. (2017). *Understanding GPS/GNSS: principles and applications.* (Artech House, Boston MA). 3rd ed.

[Levine 2021] Levine J (2021) Distributing Time and Frequency Information. Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications Volume 1, Chapter 29:821-848 (IEEE Press, Piscataway, NJ). Available at https://tf.nist.gov/general/pdf/2940.pdf

[Matsakis 2018] Matsakis D, Levine J, Lombardi, M (2018) Metrological and legal traceability of time signals. (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://tf.nist.gov/general/pdf/2941.pdf

[NASIC] National Air and Space Intelligence Center (2019) Competing in Space. (NASIC, Dayton, OH). Available at https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF

[NAVCEN] Department of Homeland Security. US Coast Guard (2020) *GPS Problem Reporting.* (DHS, USCG, Washington DC). Available at https://www.navcen.uscg.gov/contact/gps_problem_reporting

[NCCIC] Department of Homeland Security (2012) *National Cybersecurity & Communications Integration Center (NCCIC) Overview* (DHS, Washington, DC). Available at https://csrc.nist.gov/CSRC/media/Events/ISPAB-OCTOBER-2012-MEETING/documents/ispab_oct2012_lzelvin_nccic-overview.pdf

[NDAA] Department of Defense, General Services Administration, and National Aeronautics and Space Administration (2019) Interim Rule Issued by DoD, GSA, and NASA (DoD, GSA, and NASA, Washington, DC). Available at https://www.acquisition.gov/FAR-Case-2019-009/889_Part_B

[NERC CIP-008-6] North American Electric Reliability Corporation (2020) *CIP-008-6 Cyber Security Incident Reporting and Response Planning.* Available at https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf

[NERC EISAC] North American Electric Reliability Corporation (2020) *Electricity Information Sharing and Analysis Center.* Available at https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx

[NERC GRIDEX] North American Electric Reliability Corporation (2020) *GridEx.* Available at https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx

[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

[NISTIR 8014] Hastings N, Franklin, J (2015) Considerations for Identity Management in Public Safety Mobile Networks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8014. https://doi.org/10.6028/NIST.IR.8014

[NISTIR 8320] Bartock M, Souppaya M, Savino R, Knoll T, Shetty U, Cherfaoui M, Yeluri R, Malhotra, Banks D, Jordan M, Pendarakis D, Rao, JR, Romness P, Scarfone K (2022) Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases. (National Institute of Standards and Technology, Gaithersburg, MD). https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8320.pdf

[NIST JRES 120.017] Yao J, Levine J, Weiss M (2015) Toward Continuous GPS Carrier-Phase Time Transfer: Eliminating the Time Discontinuity at an Anomaly. NIST Journal of Research 120: 280-292. https://doi.org/10.6028/jres.120.017

[NIST SP 250-29] Kamas G, Lombardi, M (2004) Remote Frequency Calibrations: The NIST Frequency Measurement and Analysis Service. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 250-29, Rev. E. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication250-29e2004.pdf

[NIST SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[NIST SP 800-34] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[NIST SP 800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[NIST SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information

System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[NIST SP 800-53] Joint Task Force Transformation Initiative (2020) Security and Privacy Controls for Federal Information Systems and Organizations. (National nstitute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[NIST SP 800-61] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[NIST SP 800-1115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115

[NIST SP 800-160] Ross, R, Graubart, R, Bodeau, D, McQuaid, R (2016) Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160,Vol. 1, Rev.1. https://doi.org/10.6028/NIST.SP.800-160v1

[NIST SP 800-160-2] Ross, R, Pillitteri VY, Graubart, R, Bodeau, D, McQuaid, R (2021) Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160,Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1

[NIST SP 800-161] Boyens J, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Supply Chain Risk Management Practices for Federal Information Systems and Organizations, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161, Rev. 1. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

[NIST SP 800-184] Bartock MJ, Scarfone KA, Smith MC, Witte GA, Cichonski JA, Souppaya MP (2016) Guide for Cybersecurity Event Recovery. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-184. https://doi.org/10.6028/NIST.SP.800-184

[NIST SP 1065] Riley W, Howe DA (2008) Handbook of Frequency Stability Analysis. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1065. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50505

[NIST T&F Glossary] NIST Physical Measurement Laboratory, Time and Frequency Division (2020) *Time and Frequency Glossary from A to Z.* Available at https://www.nist.gov/pml/time-and-frequency-division/popular-links/time- frequency-z

[NIST TN 1366] Volk, CM, Levine, J (1994) Analytical Estimation of Carrier Multipath Bias on GPS Position Measurements. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Technical Note (TN) 1366. Available at http://doi.org/10.6028/NIST.TN.1366

[NIST TN 2187] Sherman JA, Arissian L, Brown RC, Deutch MJ, Donley EA, Gerginov V, Levine J, Nelson GK, Novick AN, Patla BR, Parker TE, Stuhl BK, Sutton DD, Yao J, Yates WC, Zhang V and Lombardi MA (2021) A Resilient Architecture for the Realization and Distribution of Coordinated Universal Time to Critical Infrastructure Systems in the United States. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Technical Note (TN) 2187. Available at https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2187.pdf

[NIST USNO] NIST Physical Measurement Laboratory, Time and Frequency Division (2022) NIST USNO. Available at https://www.nist.gov/pml/time-and-frequency-division/time-services/nist-usno

[NOAA SWS] NOAA Space Weather Prediction Center (2022) NOAA Space Weather Scales. Available at https://www.swpc.noaa.gov/noaa-scales-explanation

[NTP MON] Network Time Protocol (2020) *Who is using my NTP server?* Available at http://support.ntp.org/bin/view/Support/MonitoringAndControllingNTP#Who_is_using_my_NTP_server

[NTP SEC] Network Time Protocol (2020) *NTP Security Notice.* Available at http://support.ntp.org/bin/view/Main/SecurityNotice

[PPD-21] Presidential Policy Directive (PPD)-21 (2013) Critical Infrastructure Security and Resilience. (The White House, Washington, DC), DCPD201300092, February 12, 2013. https://www.govinfo.gov/content/pkg/DCPD-201300092/html/DCPD-201300092.htm

[RTCA 229] Radio Technical Commission for Aeronautics (2020) *RTCA DO-229 Minimum Operational Performance Standards for Global Positioning*

*Systems/Satellite-Based Augmentation System Airborne Equipment*. (RTCA, Washington, DC). Available at https://my.rtca.org/NC__Product?id=a1B36000001IcklEAC

[RTCA 235] Radio Technical Commission for Aeronautics (2008) *RTCA DO-235A Assessment of Radio Frequency Interference Relevant to the GNSS LI Frequency Band*. (RTCA, Washington, DC). Available at https://my.rtca.org/NC__Product?id=a1B36000001IckKEAS

[RTCA 292] Radio Technical Commission for Aeronautics (2004) *RTCA DO-292 Assessment of Radio Frequency Interference Relevant to the GNSS L5/E5A Frequency Band*. (RTCA, Washington, DC). Available at https://my.rtca.org/nc__store?search=292

[RTCA 316] Radio Technical Commission for Aeronautics (2009) *RTCA DO-316 Minimum Operational Performance Standards for Global Positioning System/Aircraft Base Augmentation System.* (RTCA, Washington, DC). Available at https://my.rtca.org/nc__store?search=316

[RTCA 326] Radio Technical Commission for Aeronautics (2010) *RTCA D DO-326 - Airworthiness Security Process Specification*. (RTCA, Washington, DC). Available at https://my.rtca.org/nc__store?search=326

[RTCA 356] Radio Technical Commission for Aeronautics (2018) *RTCA DO-356A Airworthiness Security Methods and Considerations*. (RTCA, Washington, DC). Available at https://my.rtca.org/NC Product?id=a1B36000001IcelEAC

[SEC 613] Securities Exchange Commission (2020) Rule 613 (Consolidated Audit Trail.) (SEC, Washington, DC). Available at https://www.sec.gov/divisions/marketreg/rule613-info.htm

[SNMP3] Case J et. al. Simple Network Management Protocol, Version 3 (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 3410 through (RFC) 3418. Available at https://tools.ietf.org/html/rfc3410, https://tools.ietf.org/html/rfc3411, https://tools.ietf.org/html/rfc3412, https://tools.ietf.org/html/rfc3413,https://tools.ietf.org/html/rfc3414, https://tools.ietf.org/html/rfc3415, https://tools.ietf.org/html/rfc3416, https://tools.ietf.org/html/rfc3417, https://tools.ietf.org/html/rfc3418

[SNMPSEC] Cybersecurity & Infrastructure Security Agency (2017) Reducing the Risk of SNMP Abuse. Alert (TA17-156A) (DHS, Washington, DC). Available at https://us-cert.cisa.gov/ncas/alerts/TA17-156A

[SPD-7] Space Policy Directive 7 (SPD)-7 (2021) The United States Space-Based Positioning, Navigation, and Timing Policy. (The White House, Washington, DC), DCPD-202100025, January 15, 2021. Available at

https://www.govinfo.gov/app/details/DCPD-202100025

[USG FRP] Department of Defense, Department of Homeland Security, and Department of Transportation (2021) 2021 Federal Radionavigation Plan (Department of Transportation, Washington DC). Available at https://www.transportation.gov/pnt/radionavigation-systems-planning

[USNG] Federal Geographic Data Committee (2001) Standard for A U.S. National Grid, FGDC-STD-011-2001. (FGDC, Reston, VA). Available at https://www.fgdc.gov/standards/projects/usng/TFIGURES_6.pdf/at_download/file

[USNO GPS] United States Naval Observatory (2022) GPS Time Transfer (US Navy, Washington DC). Available at https://www.cnmoc.usff.navy.mil/Organization/United-States-Naval-Observatory/Precise-Time-Department/Global-Positioning-System/USNO-GPS-Time-Transfer/

# Appendix A— Acronyms and Abbreviations

Selected acronyms and abbreviations used in this document are defined below.

| Term | Definition |
|---|---|
| CISA | Cybersecurity and Infrastructure Security Agency |
| CRPA | controlled reception patterned antenna |
| CSF | Cybersecurity Framework |
| DHS | Department of Homeland Security |
| DOT | Department of Transportation |
| EISAC | Electricity Information Sharing and Analysis Center |
| EO | Executive Order |
| FCC | Federal Communications Commission |
| FPGA | field-programmable gate array |
| GNSS | Global Navigation Satellite System |
| GPS | Global Positioning System |
| HMI | human machine interface |
| ICS | industrial control system |
| IDM | interference detection and mitigation |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IMO | International Maritime Organization |
| IMU | Inertial Measurement Units |
| INS | Inertial Navigation Systems |
| IoT | Internet of Things |
| IRIG | Inter-range Instrumentation Group Time Code |
| IRIG-B | Inter-range Instrumentation Group Time Code B |
| ISAC | Information Sharing and Analysis Center |
| ISO | International Organization for Standardization |
| ITRS | International Terrestrial Reference System |
| ITU-T | International Telecommunication Union International Telecommunications Standardization Sector |
| NANU | Notice Advisory to NAVSTAR Users |
| NASA | National Aeronautics and Space Administration |
| NAVCEN | U.S. Coast Guard Navigation Center |
| NCCIC | National Cybersecurity and Communications Integration Center |

| Term | Definition |
|---|---|
| NERC | North American Electric Reliability Corporation |
| NGS | National Geodetic Survey |
| NIST | National Institute of Standards and Technology |
| NOTAM | Notice to Airmen |
| NTP | Network Time Protocol |
| NTP SEC | NTP Security Notice |
| OEM | original equipment manufacturer |
| PII | personally identifiable information |
| PIN | personal identification number |
| PNT | positioning, navigation, and timing |
| PNT Profile | Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services |
| PPS | pulse per second |
| PTP | Precision Time Protocol |
| RAIM | receiver autonomous integrity monitoring |
| RF | radio frequency |
| RFC | request for comments |
| RFI | radio frequency interference |
| RTO | recovery time objectives |
| SCADA | Supervisory Control and Data Acquisition |
| SLA | service-level agreement |
| SP | Special Publication |
| SPS | Standard Positioning Service |
| TBS | Terrestrial Beacon System |
| USG FRP | U.S. Government Federal Radionavigation Plan |
| USNO | United States Naval Observatory |
| UTC | Coordinated Universal Time |
| VPN | virtual private network |
| WAAS | Wide Area Augmentation System |
| WLAN | wireless local area network |
| WGS-84 | World Geodetic System – 1984 |

# Appendix B— Glossary

Selected terms used in this document are defined below.

**Accuracy (Absolute):** The degree of conformity of a measured or calculated value to the true value, typically based on a global reference system. For time, the global reference can be based on the following time scales: UTC, TAI, or GPS. For position, the global reference can be WGS-84.

**Accuracy (Relative):** The degree of agreement between measured or calculated values among the devices and applications dependent on the position, navigation, or time data at an instant in time.

**Agility:** The property of a system or an infrastructure that can be reconfigured, in which resources can be reallocated, and in which components can be reused or repurposed so that cyber defenders can define, select, and tailor cyber courses of action for a broad range of disruptions or malicious cyber activities. [NIST SP 800-160]

**Allan deviation:** A non-classical statistic used to estimate stability. The NIST equation for the Allan deviation (with non-overlapping samples) is

$$\sigma_y(\tau) = \sqrt{\frac{1}{2(M-1)}\sum_{i=1}^{M-1}(\bar{y}_{i+1} - \bar{y}_i)^2}$$

where $\bar{y}_i$ is the $i^{\text{th}}$ of $M$ frequency offset averages over the observation period, $\tau$. Or

$$\sigma_y(\tau) = \sqrt{\frac{1}{2\tau^2(N-2)}\sum_{i=1}^{N-2}(x_{i+2} - 2x_{i+1} + x_i)^2}$$

where $x_i$ is a series of phase offset measurements in time units that consists of individual measurements, $x_1,\ x_2,\ x_3$, and so on, $N$ is the number of values in the $x_i$ series, and the data are equally spaced in intervals τ seconds long.

The confidence interval of an Allan deviation estimate is dependent on the noise type but is often estimated as $\frac{\sigma_y(\tau)}{\sqrt{N}}$. [NIST T&F Glossary, Adapted] [NIST SP 1065, Adapted]

**Atomic Clock:** A clock referenced to an atomic oscillator. Only clocks with an internal atomic oscillator qualify as atomic clocks. [NIST T&F Glossary, Adapted]

**Atomic Oscillator:** An oscillator that uses the quantized energy levels in atoms or molecules as the source of its resonance. The laws of quantum mechanics dictate that the energies of a bound system, such as an atom, have certain discrete values. An electromagnetic field at a particular frequency can boost an atom from one energy level to a higher one, or an atom at a high energy level can drop to a lower level by emitting energy. The resonance frequency, $f_o$, of an atomic oscillator is the difference between the two energy levels divided by Planck's constant, $h$.

The principle underlying the atomic oscillator is that since all atoms of a specific element are

identical, they should produce exactly the same frequency when they absorb or release energy. In theory, the atom is a perfect "pendulum" whose oscillations are counted to measure a time interval. The national frequency standards developed by NIST and other laboratories derive their resonance frequency from the cesium atom and typically use cesium fountain technology. Rubidium oscillators are the lowest priced and most common atomic oscillators, but cesium beam and hydrogen maser atomic oscillators are also sold commercially in much smaller quantities. [NIST T&F Glossary]

**Attack:** Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [CNSSI 4009]

**Availability (PNT):** The availability of a PNT system is the percentage of time that the services of the system are usable. Availability is an indication of the ability of the system to provide usable service within the specified coverage area. Signal availability is the percentage of time that PNT signals transmitted from external sources are available for use. Availability is a function of both the physical characteristics of the environment and the technical capabilities of the PNT service provider. [USG FRP Appendix E, Adapted]

**Calibration:** A comparison between a device under test and an established standard, such as UTC(NIST). When the calibration is finished, it should be possible to state the estimated time offset and/or frequency offset of the device under test with respect to the standard, as well as the measurement uncertainty. Calibrations can be absolute or relative. Absolute calibrations are not biased by the calibration reference and would, therefore, be more reproducible. However, absolute calibrations can be more complex to determine. The bias in relative calibrations would be consistent if all the devices in the system are calibrated against the same calibration reference. Calibrations may also be performed relative to other devices without reference to an absolute standard. Relative calibrations are generally simpler to perform than absolute calibrations. [NIST T&F Glossary, Adapted]

**Characterization:** An extended test of the performance characteristics of a clock or oscillator. A characterization involves more work than a typical calibration. The device under test is usually measured for a long period of time (days or weeks), and sometimes, a series of measurements is made under different environmental conditions. A characterization is often used to determine the types of noise that limit the uncertainty of the measurement and the sensitivity of the device to environmental changes. [NIST T&F Glossary]

**Clock:** A device that generates periodic, accurately spaced signals for timekeeping applications. A clock consists of at least three parts: an oscillator, a device that counts the oscillations and converts them to units of time interval (such as seconds, minutes, hours, and days), and a means of displaying or recording the results. [NIST T&F Glossary]

**Component:** A hardware, software, firmware part or element of a larger PNT system with well-defined inputs and outputs and a specific function. [NIST SP 800-160, Adapted][DHS RCF, Adapted]

**Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST FIPS 200]

**Continuity:** The probability that the specified PNT system performance will be maintained for the duration of a phase of operation, presuming that the PNT system was available at the beginning of that phase of operation. [USG FRP]

**Coverage:** The surface area or space volume in which the signals are adequate to permit the user to determine a position to a specified level of accuracy. Coverage is influenced by system geometry, signal power levels, receiver sensitivity, atmospheric noise conditions, and other factors that affect signal availability. [USG FRP]

**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]

**Delay (Path Delay):** The [signal] delay between a transmitter and a receiver. Path delay is often the largest contributor to time transfer uncertainty. For example, consider a radio signal broadcast over a 1000 km path. Since radio signals travel at the speed of light (with a delay of about 3.3 μs/km), we can calibrate the 1000 km path by estimating the path delay as 3.3 ms and applying a 3.3 ms correction to our measurement. Sophisticated time transfer systems, such as GPS, automatically correct for path delay. The absolute path delay is not important to frequency transfer systems because on-time pulses are not required, but variations in path delay still limit the frequency uncertainty. [NIST T&F Glossary, Adapted]

**Disciplined Oscillator (DO):** An oscillator whose output frequency is continuously adjusted (often through the use of a phase locked loop) to agree with an external reference. For example, a GPS disciplined oscillator (GPSDO) usually consists of a quartz or rubidium oscillator whose output frequency is continuously adjusted to agree with signals broadcast by the GPS satellites.

**Frequency:** The rate of a repetitive event. If $T$ is the period of a repetitive event, then the frequency $f$ is its reciprocal, $1/T$. Conversely, the period is the reciprocal of the frequency, $T = 1 / f$. Because the period is a time interval expressed in seconds (s), it is easy to see the close relationship between time interval and frequency. The standard unit for frequency is the hertz (Hz), defined as the number of events or cycles per second. The frequency of electrical signals is often measured in multiples of hertz, including kilohertz (kHz), megahertz (MHz), or gigahertz (GHz). [NIST T&F Glossary]

**Frequency Accuracy:** The degree of conformity of a measured or calculated frequency to its definition. Because accuracy is related to the offset from an ideal value, frequency accuracy is usually stated in terms of the frequency offset. [NIST T&F Glossary]

**Frequency Drift:** An undesired progressive change in frequency with time. Frequency drift can be caused by instability in the oscillator and environmental changes, although it is often hard to distinguish between drift and oscillator aging. Frequency drift may be in either direction (resulting in a higher or lower frequency) and is not necessarily linear. [NIST T&F Glossary]

**Frequency Offset:** The difference between a measured frequency and an ideal frequency with

zero uncertainty. This ideal frequency is called the nominal frequency. [NIST T&F Glossary]

Frequency offset can be measured in either the frequency domain or the time domain. A simple frequency domain measurement involves directly counting and displaying the output frequency of the device under test with a frequency counter. The frequency offset is calculated as

$$f_{off} = \frac{f_{meas} - f_{nom}}{f_{nom}}$$

where $f_{meas}$ is the reading from the frequency counter, and $f_{nom}$ is the specified output frequency of the device under test.

Frequency offset measurements in the time domain involve measuring the time difference between the device under test and the reference. The time interval measurements can be made with an oscilloscope or a time interval counter. If at least two time interval measurements are made, frequency offset can be estimated as

$$f_{off} = -\frac{\Delta t}{T}$$

where $\Delta t$ is the difference between time interval measurements (phase difference), and $T$ is the measurement period. [NIST T&F Glossary, Adapted]

**Frequency Stability:** The degree to which an oscillating signal produces the same frequency for a specified interval of time. It is important to note the time interval—some devices have good short-term stability while others have good long-term stability. Stability does not determine whether the frequency of a signal is right or wrong. It only indicates whether that frequency stays the same. The Allan deviation is the most common metric used to estimate frequency stability, but several similar statistics are also used. [NIST T&F Glossary]

**Global Navigation Satellite System (GNSS):** GNSS collectively refers to the worldwide positioning, navigation, and timing (PNT) determination capability available from one or more satellite constellations. Each GNSS system employs a constellation of satellites that operate in conjunction with a network of ground stations. Receivers and system integrity monitoring are augmented as necessary to support the required position, navigation, and timing performance for the intended operation. [USG FRP, Adapted] [ICAO 9849, Adapted]

**GPS:** The Global Positioning System (GPS) is a U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services. This system consists of three segments: the space segment, the control segment, and the user segment. The U.S. Space Force develops, maintains, and operates the space and control segments. [GPS GNSS]

**Holdover:** An operating condition of a clock which has lost its controlling reference input, is using its local oscillator, and can be augmented with stored data acquired while locked to the reference input or a frequency reference to control its output.

**Integrity:** A measure of the trust that can be placed in the correctness of the information supplied by a PNT service provider. Integrity includes the ability of the system to provide timely

warnings to users when the PNT data should not be used. [USG FRP]

**Interchangeable:** The ability to combine signals from multiple PNT data sources into a single PNT solution, as well as the ability to provide a solution from an alternative source when a primary source is not available. [USG FRP]

**Interference (electromagnetic):** Any electromagnetic disturbance that interrupts, obstructs, degrades, or otherwise limits the performance of user equipment. [USG FRP, Appendix E]

**Jamming (electromagnetic):** The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing the effective use of a signal. [USG FRP, Appendix E]

**Jitter:** The short-term variations of the significant instants of a timing signal from their ideal positions in time (where short-term implies that these variations are of frequency greater than or equal to 10 Hz). [ITU-T 810]

**Leap Second:** A second added to Coordinated Universal Time (UTC) to make it agree with astronomical time to within 0.9 second. UTC is an atomic time scale based on the performance of atomic clocks. Astronomical time is based on the rotational rate of the Earth. Since atomic clocks are more stable than the rate at which the Earth rotates, leap seconds are needed to keep the two time scales in agreement. [NIST T&F Glossary, Adapted]

**Multipath:** The propagation phenomenon that results in signals reaching the receiving antenna by two or more paths. When two or more signals arrive simultaneously, wave interference results. The received signal fades if the wave interference is time varying or if one of the terminals is in motion. [USG FRP, Appendix E]

**Navigation:** The ability to determine a current and desired position (relative or absolute) and apply corrections to course, orientation, and speed to attain a desired position. Navigation coverage requirements could be global, from sub-surface to surface and from surface to space. [DOT, Adapted]

**Nominal Frequency:** An ideal frequency with zero uncertainty. The nominal frequency is the frequency labeled on an oscillator's output. For this reason, it is sometimes called the nameplate frequency. For example, an oscillator whose nameplate or label reads 5 MHz has a nominal frequency of 5 MHz. The difference between the nominal frequency and the actual output frequency of the oscillator is the frequency offset. [NIST T&F Glossary]

**Oscillator:** An electronic device used to generate an oscillating signal. The oscillation is based on a periodic event that repeats at a constant rate. The device that controls this event is called a resonator. The resonator needs an energy source so it can sustain oscillation. Taken together, the energy source and resonator form an oscillator. Although many simple types of oscillators (both mechanical and electronic) exist, the two types of oscillators primarily used for time and frequency measurements are quartz oscillators and atomic oscillators. [NIST T&F Glossary]

**PNT Data:** All information used to form or disseminate PNT solutions, including signals, waveforms, and network packets.

**PNT Solution:** The full solution provided by a PNT system or source, including time, position, and velocity. A PNT system or source may provide a full PNT solution or a part of it. For example, a GNSS receiver provides a full PNT solution, while a local clock provides only a timing or frequency solution. [DHS RCF]

**PNT Source:** A PNT system component that is used to produce a PNT solution. Examples include GNSS receivers, networked and local clocks, inertial navigation systems (INS), and timing services provided over a wired or wireless connection. [DHS RCF]

**PNT System:** The components, processes, and parameters that collectively produce the final PNT solution for the consumer. [DHS RCF]

**Phase:** The position of a point in time (instant) on a waveform cycle. A complete cycle is defined as the interval required for the waveform to retain its arbitrary initial value. [NIST T&F Glossary]

**Phenomenologies:** Physical phenomena such as radio frequencies, inertial sensors, and scene mapping, as well as diverse sources and data paths using those physical phenomena (e.g., multiple radio frequencies) to provide interchangeable solutions to users to ensure robust availability. [USG FRP]

**Positioning:** The ability to accurately and precisely determine one's location and orientation two-dimensionally (or three-dimensionally, when required) referenced to a standard reference frame, such as the World Geodetic System 1984, WGS84[G873], or ITRF2014. [DOT]

**Precision:** Refers to how closely individual PNT measurements agree with each other. [USG FRP]

**Proper Working State:** A condition in which the device or system contains no compromised internal components or data fields (e.g., data stored to memory) and from which the device or system can recognize and process valid input signals and output valid PNT solutions. An initial pre-deployment configuration is a basic example. The accuracy of the immediate PNT solution is not specified in this definition, as it will depend on the specifics of the device or system's performance and the degradation allowed by different resilience levels. [DHS RCF]

**Reliability:** The probability of performing a specified function without failure under given conditions for a specified period of time. [USG FRP]

**Residual Risk:** Portion of risk remaining after security measures have been applied. [CNSSI 4009]

**Resilience:** The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. [PPD-21]

**Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST SP 800-37]

**Risk Assessment:** The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. [NIST SP 800-30]

**Risk Management:** The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation and includes (i) establishing the context for risk-related activities, (ii) assessing risk, (iii) responding to risk once determined, and (iv) monitoring risk over time. [NIST SP 800-39]

**Risk Management Framework:** The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. [NIST SP 800-37]

**Secure:** To reduce the risks of intrusions and attacks as well as the effects of natural or manmade disasters on critical infrastructure by physical means or defensive cyber measures. [PPD-21]

**Short-Term Stability:** The stability of a time or frequency signal over a short measurement interval, usually an interval of 100 seconds or less in duration. [NIST T&F Glossary]

**Stability:** An inherent characteristic of an oscillator that determines how well it can produce the same frequency over a given time interval. Stability does not indicate whether the frequency is right or wrong, but only whether it stays the same. The stability of an oscillator does not necessarily change when the frequency offset changes. An oscillator can be adjusted, and its frequency moved either further away from or closer to its nominal frequency without changing its stability at all.

The stability of an oscillator is usually specified by a statistic, such as the Allan deviation, that estimates the frequency fluctuations of the device over a given time interval. Some devices, such as an OCXO [Oven Controlled Crystal (Xtal) Oscillator] have good short-term stability and poor long-term stability. Other devices, such as a GPS disciplined oscillator (GPSDO), typically have poor short-term stability and good long-term stability. [NIST T&F Glossary, Adapted]

**Synchronization:** The process of setting two or more clocks to the same time. [NIST T&F Glossary]

**Syntonization:** The process of setting two or more oscillators to the same frequency. [NIST T&F Glossary]

**Threat:** Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, or denial of service. [NIST SP 800-53]

**Traceability, Metrological:** Property of a measurement result whereby the result can be related

to a reference through a documented, unbroken chain of calibrations, each contributing to the measurement uncertainty. [VIM]

**Time Interval:** The elapsed time between two events. In time and frequency metrology, time interval is usually measured in small fractions of a second, such as milliseconds, microseconds, or nanoseconds. Higher resolution time interval measurements are often made with a time interval counter. [NIST T&F Glossary]

**Time Scale:** An agreed upon system for keeping time. All time scales use a frequency source to define the length of the second, which is the standard unit of time interval. Seconds are then counted to measure longer units of time interval, such as minutes, hours, or days. Modern time scales, such as UTC, define the second based on an atomic property of the cesium atom, and thus standard seconds are produced by cesium oscillators. Earlier time scales (including earlier versions of Universal Time) were based on astronomical observations that measured the frequency of the Earth's rotation. [NIST T&F Glossary]

**Validation:** Confirmation (through the provision of strong, sound, and objective evidence and demonstration) that requirements for a specific intended use or application have been fulfilled and that the system, while in use, fulfills its mission or business objectives while being able to provide adequate protection for stakeholder and mission or business assets, minimize or contain asset loss and associated consequences, and achieve its intended use in its intended operational environment with the desired level of trustworthiness. [NIST SP 800-160, §3.4.11, Adapted]

**Verification:** Process of producing objective evidence that sufficiently demonstrates that the system satisfies its security requirements and security characteristics with the level of assurance that applies to the system. [NIST SP 800-160, §3.4.9, Adapted]

**Vulnerability:** A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [NIST SP 800-30]

**Wander:** The long-term variations—random walk frequency noise—of the significant instants of a digital signal from their ideal position in time (where long-term implies that these variations are of frequency less than 10 Hz). [ITU-T 810, Adapted]

**World Geodetic System 1984 (WGS 84):** An Earth-centered, Earth-fixed terrestrial reference system and geodetic datum. WGS 84 is based on a consistent set of constants and model parameters that describe the Earth's size, shape, gravity, and geomagnetic fields. WGS 84 is the standard U.S. Department of Defense definition of a global reference system for geospatial information and is the reference system for GPS. It is consistent with the International Terrestrial Reference System (ITRS). [USG FRP]

# Appendix C—Additional Resources

3rd Generation Partnership Project (2020) *3GPP TS 22.104 Service Reequipments for Cyber-physical Control Applications in Vertical Domains.* (3GPP, Sophia Antipolis, France). Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3528

3rd Generation Partnership Project (2018) *R2-1817172 Overview of UE Time Synchronization Methods.* (3GPP, Sophia Antipolis, France). Available at https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_104/Docs/R2-1817172.zip

3rd Generation Partnership Project (2020) *SID: Feasibility Study on 5G Timing Resiliency System FS_5TRS.* (3GPP, Sophia Antipolis, France). Available at https://portal.3gpp.org/ngppapp/CreateTDoc.aspx?mode=view&contributionUid=S1-202281

https://www.afrl.af.mil/News/Article/2874807/afrls-pnt-agilepod-achieves-flight-test-objectives/https://doi.org/10.21236/ADA290597 or https://afresearchlab.com/technology/sensors/agilepod/

ATIS (2017) *ATIS-0900005 GPS Vulnerability*. (ATIS, Washington, DC). Available at https://access.atis.org/apps/group_public/download.php/36304/ATIS-0900005.pdf

Allan DW, Weiss MA (1980) Accurate Time and Frequency Transfer During Common-View of a GPS Satellite, *34th Annual Frequency Control Symposium*, (U.S. Army Electronic Research and Development Command, Philadelphia, PA) pp. 334-346. Available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a213670.pdf

Anand DM, Freiheit C, Weiss, MA, Shenoi K, Ossareh H (2019) A Timing Impairment Module for Electrical Synchrometrology. *2019 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, (IEEE, Portland, OR), pp. 1-7. Available at https://ieeexplore.ieee.org/document/8886638

Boehm BW (1991) Software risk management: Principles and practices. *IEEE Software*, vol. 8, no.1, pp. 32–41. Available at https://doi.org/10.1109/52.62930

Communications Security, Reliability, And Interoperability Council VII (2020) Final Report - Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation. *(Working Group 2: Managing Security Risk in the Transition to 5, CSRIC, Washington, DC).* Available at https://www.fcc.gov/file/18918/download

CTIA (2019) Protecting America's Next-Generation Networks (CTIA, Washington, DC). Available at https://api.ctia.org/wp- content/uploads/2018/07/ProtectingAmericasNetworks_FINAL.pdf

Department of Defense. (2015) *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*. (DOD, Washington, DC). Available at https://www.dau.edu/tools/Lists/DAUTools/Attachments/37/DoD%20-

%20Guidebook,%20Cybersecurity%20Risk%20Management%20Framework,%20v1.08,%20Sep%202015.pdf

Dropping B, Coggins K, Platt J. (2018) Timing Security: Mitigating Threats in a Changing Landscape Webinar. (ATIS, Washington, DC). Available at https://www.atis.org/wp-content/uploads/01_news_events/webinar-pptslides/Timing-Security5222018.pdf

Egea-Roca D, Arizabaleta-Diez M, Pany T, Antreich F, Lopez-Salcedo JA, Paonni M, Seco-Granados G (2022) GNSS User Technology: State-of-the-Art and Future Trends. *IEEE Access*, vol. 10, pp.39939–39968. Available at https://doi.org/10.1109/ACCESS.2022.3165594

Electric Power Research Institute (2020) Roadmap for Resilient Positioning, Navigation, and Timing (PNT) For the Electricity Subsector. (EPRI, Washington, DC). Available at https://www.epri.com/research/products/000000003002020266

European Securities and Markets Authority (2017) Guidelines Transaction Reporting, Order Record Keeping and Clock Synchronisation Under MiFID II. (EMSA, Lison, Portugal). Available at https://www.esma.europa.eu/sites/default/files/library/2016-1452_guidelines_mifid_ii_transaction_reporting.pdf

Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013. Available at https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf

Federal Aviation Administration, Department of Transportation (2020) *NOTAMS, TFRs, Aircraft Safety Alerts* (Department of Transportation, Washington, DC). Available at https://www.faa.gov/pilots/safety/notams_tfr/

Federal Aviation Administration, U.S. Department of Transportation (2020) *Wide Area Augmentation System.* Available at https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/library/factsheets/media/WAAS_QFSheet.pdf

Federal Aviation Administration, U.S. Department of Transportation (2020) *SBAS Worldwide.* Available at https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/Gnss/library/factSheets/media/SBAS_Worldwide_QFact.pdf

Federal Trade Commission (2020) *Jammer Enforcement.* (FCC, Washington, DC). Available at https://www.fcc.gov/general/jammer-enforcement

Hopkin P (2018) Fundamentals of risk management: Understanding, evaluating and implementing effective risk management. Kogan Page Publishers. Available at http://dspace.vnbrims.org:13000/xmlui/bitstream/handle/123456789/5077/Fundamentals%20of%20Risk%20Management.pdf?sequence=1

International Maritime Organization (2002) IMO Resolution A.915(22) Revised Maritime Policy and Requirements for a Future GNSS. (IMO, London, England). Available at

https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.915(22).pdf

International Organization for Standardization (2018) ISO 31000:2018 – Risk management – Guidelines (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/65694.html

International Organization for Standardization/International Electrotechnical Commission (2018) ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/75281.html

Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

Haimes, Y. Y., Kaplan, S., & Lambert, J. H. (2002). Risk filtering, ranking, and management framework using hierarchical holographic modeling. Risk Analysis, 22(2), 383-397.

Lambert JH, Keisler JM, Wheeler WE, Collier ZA, Linkov I (2013). Multiscale approach to the security of hardware supply chains for energy systems. *Environment Systems and Decisions*, vol. 33 no.3, pp.326-334. Available at https://doi.org/10.1007/s10669-013-9465-2

Levine J (1999) Introduction to time and frequency metrology. *Review of scientific instruments* 70(6):2567-2596. Available at https://tf.nist.gov/general/pdf/1288.pdf

Levine J (2016) Measuring Time and Comparing Clocks. (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://tf.nist.gov/general/pdf/2718.pdf

Linkov I, Bridges T, Creutzig F, Decker J, Fox-Lent C, Kröger W, Lambert JH, Levermann A, Montreuil B, Nathwani J, Nyer R (2014) Changing the resilience paradigm. Nature Climate Change. vol.4, no. 6, pp.407-9.

National Institute of Standards and Technology (2020) *NIST Time Calibration Services.* (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://www.nist.gov/programs-projects/time-measurement-and-analysis-service-tmas

National Oceanic and Atmospheric Association (2020) *National Geodetic Survey. Antenna Calibrations.* (NOAA, Washington, DC). Available at https://www.ngs.noaa.gov/ANTCAL/

Nighswander T, Ledvina B, Diamond J, Brumley R, Brumley D (2012) GPS Software Attacks. *Proceedings of the 2012 ACM Conference on Computer and Communications Security.* (Association for Computer Machinery, Raleigh, NC), pp. 450-461. https://dl.acm.org/doi/10.1145/2382196.2382245

North American Electrical Reliability Corporation (2020) *Reliability Standards for the Bulk Electric Systems of North America, Standard BAL-001-2 – Real Power Balancing Control Performance*. (NERC, Washington, DC). Available at https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.

pdf

Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179. https://doi.org/10.6028/NIST.IR.8179

Plumb J, Larson KM, White J, Powers E (2005) Absolute calibration of a geodetic time transfer system. *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control* 52(11):1904-11. Available at https://ieeexplore.ieee.org/abstract/document/1561658

Psiaki M, Humphreys T (2016) GNSS Spoofing and Detection. *Proceedings of the IEEE,* (IEEE, Piscataway, NJ), pp 1258-1270.

Savory J, Sherman J, Romisch S (2018) White rabbit-based time distribution at NIST. *IEEE International Frequency Control Symposium (IFCS)* (IEEE, Piscataway, NJ), pp. 1-5. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=925954

Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2

Sullivan DB, Allan DW, Howe DA, Walls FL eds. (1990) Characterization of Clocks and Oscillators. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Technical Note (TN) 1337. https://doi.org/10.6028/NIST.TN.1337

University of Texas (2020) *Texas Spoofing Test Battery (TEXBAT).* (University of Texas, Austin, TX). Available at https://radionavlab.ae.utexas.edu/index.php?option=com_content&view=article&id=289:texas-spoofing-test-battery-texbat&catid=50&Itemid=27

Lombardi MA (2002) Fundamentals of Time and Frequency. *The Mechatronics Handbook*. Available at https://tf.nist.gov/general/pdf/1498.pdf

Lombardi MA (2010) A NIST disciplined oscillator: Delivering UTC (NIST) to the calibration laboratory. *NCSLi Measure* 5(4):46-54. Available at https://tf.nist.gov/general/pdf/2478.pdf

Lombardi MA, Nelson LM, Novick AN, Zhang VS (2001) Time and Frequency Measurements Using the Global Positioning System. *Cal. Lab. Int. J. Metrology* July-September:26-33. Available at https://tf.nist.gov/general/pdf/1424.pdf

Mader GL (1999) GPS antenna calibration at the National Geodetic Survey. *GPS solutions*3(1):50-8. https://link.springer.com/article/10.1007/PL00012780

Morton YJ, van Diggelen F, Spilker Jr JJ, Parkinson BW, Lo S, Gao G (2021) Position, Navigation, and Timing Technologies in the 21st Century, Volumes 1 and 2: Integrated Satellite Navigation, Sensor Systems, and Civil Applications. (IEEE Press, Piscataway, NJ). Available at

https://ieeexplore.ieee.org/book/9304973

NASPI Time Synchronization Task Force (2017) *Time Synchronization in the Electric Power System. NASPI Technical Report.* (North American Synchrophasor Initiative). Available at https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf

National Emergency Number Association (2016) *NENA-STA-026.5 NENA PSAP Master Clock Standard* (NENA, Alexandria, VA). Available at https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-STA-026.5- 2016_PSAP_Mas.pdf

National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

National Institute of Standards and Technology (2020) *NIST Frequency Calibration Services.* (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://www.nist.gov/programs-projects/frequency-measurement-and-analysis-service-fmas

National Institute of Standards and Technology (2020) *NIST Internet Time Service.* (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://www.nist.gov/time-distribution/internet-time-service-its

Wang F, Li H, Lu M (2017) GNSS Spoofing Detection and Mitigation Based on Maximum Likelihood Estimation. *Sensors,* 17:1532.

Wong E. (2020) Responsible Use of PNT for DLT in the Financial Services Sector ATIS Time and Money Conference (New York, NY). Available at https://www.gps.gov/multimedia/presentations/2020/ATIS/wong.pdf

Yao J, Lombardi MA, Novick N, Patla B, Sherman JA, Zhang VS. (2016) The Effects of the January 2016 UTC Offset Anomaly on GPS-Controlled Clocks Monitored At NIST. (National Institute of Standards and Technology, Gaithersburg, MD.) Available at https://tf.nist.gov/general/pdf/2886.pdf

Yao J, Weiss M, Curry C, Levine J (2016) GPS Jamming and GPS Carrier-Phase Time Transfer. *Proceedings of the 2016 Precise Time and Time Interval Meeting, ION-PTTI 2016* (Monterey CA), pp 80-85. Available at https://www.nist.gov/publications/gps-jamming-and-gps-carrier-phase-time-transfer

# Appendix D—Applying the PNT Profile to Cybersecurity Risk Management

The PNT Profile can be used to augment any risk management framework. This section further tailors the PNT Profile in context of a few fault scenarios. An effective PNT risk management strategy provides a dynamic and flexible approach to control risks in evolving environments. A comprehensive risk management strategy requires proper preparation, which is further detailed in Appendix E. Organizations are encouraged to apply the PNT Profile with their risk management framework from concept to acquisitions to acceptance, integration and deployment, to operations and maintenance.

Each organization selects PNT Profile sub-categories, the cybersecurity outcomes relevant to their mission and business objectives, and implements associated controls proportional to their risk exposure. The organization verifies and validates the implementation throughout the PNT system lifecycle. A comprehensive, well-documented, and disciplined risk management process for PNT systems allows for continuous monitoring of threats, likelihoods, and impacts, in order to provide efficient identification and analysis of risks and effectiveness of the controls applied to manage those risks. Equally important, an agile risk management approach enables continuous adaptation to evolving threats through adoption of innovative and rapid advances in technology and current best practices.

Table 25 illustrates how the PNT Profile is used by a notional organization to address example scenarios and apply the five functions of the CSF to manage the risk to PNT systems.

1660 **Table 25 - Applying the PNT Profile to User Risk Management**

| Example Scenarios | Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|---|
| **User:** A human action or inaction with a system resulting in faults or failure in the PNT system or data. User risks include both unintentional and intentional threats. | *Identify personnel qualifications and user equipment training.* Baseline personnel qualifications and training on designing, deploying, testing, securing, and maintaining PNT user equipment are implemented and verified. [AM-1 through AM-5]<br><br>*Identify vulnerabilities and threats* related to personnel integrating, maintaining, and relying on PNT user equipment and services. [RA-1, RA-2, RA-3] | Awareness and adherence to *installation and maintenance best practices*. [IP-1, MA-1, MA-2]<br><br>*Configuration change control process* are established and adhered to. [IP-3]<br><br>Enable event logging including identification of users and components associated with an event. [PT-1]<br><br>Assure sound systems engineering and integration and administration teams have *adequate cybersecurity, user equipment, testing, and maintenance training*. User have training and experience in using complementary sources of PNT data and signals. [AT-2]<br><br>Understand *user responsibilities* with respect to PNT data performance. [AT-3]<br><br>*User identities are securely managed* with access control | *End-to-end systems testing* to verify user configuration after firmware, software, equipment integration and upgrades. [DS-4]<br><br>Newly deployed or updated PNT data streams are continuously monitored against established PNT data sources to correlate faults. [AE-3]<br><br>PNT data alert thresholds are established. [AE-5]<br><br>*Integrity monitoring*. Continuous monitoring of user actions and related risk management controls. [CM-1] | *Execute response plan.* Apply proper working configuration. Document steps and results and address changes relative to user interactions with the PNT system, in addition to any software and hardware configuration changes, in the response plan. Record new threats and vulnerabilities. [RP-1, MI-2, MI-3]<br><br>Continue to *log data* from all PNT sources as feasible. [AN-1]<br><br>*Operational constraints* due to loss or compromise of the PNT data are *understood and communicated* before continuing operations.[ AN-2]<br><br>*Alert stakeholders* including downstream users describing the limitations and extent of disruption in PNT | *Execute recovery plan.* Restore PNT system within an acceptable time period. Perform system acceptance testing.The recovery plan can include specific actions for restoration, recalibration, resetting, and test validation of equipment. [RP-1]<br><br>*Periodically verify personnel are adequately trained* to execute recovery plans. [CO-1]<br><br>*Update risk assessment.* Improve PNT training, testing, monitoring, detection, response, recovery procedures, and resiliency features. [IM-1]<br><br>*Update the recovery plan* to incorporate lessons learned, reflect new threats, improve technology, and address changes to the organization, PNT system, operating |

| Example Scenarios | Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|---|
| | | limited to their roles and responsibilities. [AC-1, AC-4, AC-6, AC-7] | | source integrity and availability. [CO-2, CO-3] | environment, and problems encountered during plan implementation, execution, and testing. [IM-2] |
| **Software:** Fault or failure in the PNT user equipment firmware or application code and associated impact on other systems that are dependent on the software. The faults or failures encompass unintentional performance degradation due to malicious breaches. | *Inventory software applications producing or relying on PNT data or signals.* PNT software and intended use, users, applicable regulations, and environment, including baseline performance characteristics, performance limitations are understood and verified. [AM-1 through AM-5]<br><br>*Identify vulnerabilities and threats* to PNT user software and downstream applications. [RA-1, RA-2, RA-3] | A baseline software configuration adhering to cybersecurity principles for applications providing and using PNT data is applied. [IP-1]<br><br>Systematic calibration and characterization procedures of PNT system uncertainty and integrity alert thresholds. [MA-1]<br><br>*End-to-end systems testing* to verify firmware, software, equipment integration and upgrades. [DS-4]<br><br>Adopt appropriate software assurance methods including but not limited to *standards*, *conformance test methods*, and *certification processes* needed to meet organizational requirements. [DS-6]<br><br>Firmware and software updates are verified to | *Event logging* including both normal and anomalous software operating states. [AE-3]<br><br>PNT data *alert thresholds* are established. [AE-5]<br><br>*Integrity monitoring.* Continuous monitoring of the PNT device outputs and applications relying on the PNT data from the device and associated risk management controls. [CM-1] | *Execute response plan.* Notify downstream users of potential PNT data availability and integrity impacts. Apply proper working configuration.Document steps and results and address changes in software or software configuration with the PNT system in the response plan. Record new threats and vulnerabilities. [RP-1, MI-1, MI-2, MI-3]<br><br>Continue to *log data* from all PNT sources as feasible. [AN-1]<br><br>*Operational constraints* due to loss or compromise of the PNT data are *understood and communicated* before continuing operations.[ | *Execute recovery plan.* Restore PNT system within an acceptable time period. Perform system acceptance testing.The recovery plan can include specific actions for restoration, recalibration, resetting, and test validation of equipment. [RP-1]<br><br>*Update risk assessment.* Improve PNT training, testing, monitoring, detection, response, recovery procedures, and resiliency features. [IM-1]<br><br>*Update the recovery plan* to incorporate lessons learned, reflect new threats, improve technology, and address changes to the organization, PNT system, operating |

| Example Scenarios | Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|---|
| | | conform to standards and to understand impact of changes on user applications. Backup configuration files of known proper working states. [IP-3]<br><br>Enable event logging including both normal and anomalous software operating states. [PT-1] | | AN-2]<br><br>*Alert stakeholders* including the device manufacturer about hardware faults or failures describing the limitations and extent of disruption in PNT source integrity. [CO-2, CO-3] | environment, and problems encountered during plan implementation, execution, and testing. [IM-2] |
| **Hardware**: Fault or failure in the PNT user equipment design, or implementation or integration, such as gateware. | *Inventory all physical devices.* PNT user equipment and intended use, users, applicable regulations, and environment, including baseline performance characteristics are understood and verified. [AM-1 through AM-5]<br><br>*Identify vulnerabilities and threats* to PNT devices and components. [RA-1, RA-2, RA-3]<br><br>*Identify hardware resilience capabilities.* Consider how other sensors can be leveraged to monitor and detect anomalies in PNT sources. [BE-5] | *Calibration and characterization of PNT system uncertainty* including establishment of testing, certification, and continuous monitoring and integrity alert thresholds expectations under operational environmental conditions. [MA-1]<br><br>*Event logging* including both normal and anomalous hardware operating states. [PT-1]<br><br>*Redundancy* or *complementary sensors and sensor fusion algorithms.* User equipment technologies: Holdover clocks, inertial measurement/navigation systems, simultaneous localization and mapping, and | *Integrity monitoring.* Continuous monitoring of the PNT user equipment and associated components including effectiveness of mitigation controls. [CM-1]<br><br>*Event logging* including both normal and anomalous hardware operating states. [AE-3]<br><br>PNT data *alert thresholds* are established. [AE-5]<br><br>*Verify PNT device integrity and availability*. Identify and document known limitations. [DS-1, DS- | *Execute response plan.* Notify downstream users of potential PNT data availability and integrity impacts. Apply proper working configuration.Document steps and results and address changes in hardware or hardware configuration with the PNT system in the response plan. Record new threats and vulnerabilities. [RP-1, MI-1, MI-2, MI-3]<br><br>Continue to *log data* from all PNT sources as feasible. [AN-1]<br><br>*Operational constraints* due to loss or | *Execute recovery plan.* Restore PNT system within an acceptable time period. Perform system acceptance testing.The recovery plan can include specific actions for restoration, recalibration, resetting, and test validation of equipment. *Verify backup PNT sources* are serviceable, operational, and sufficient before continuing operations safely. [RP-1]<br><br>*Update risk assessment.* Improve PNT training, testing, monitoring, detection, response, recovery procedures, and resiliency features. [IM- |

| Example Scenarios | Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|---|
| | | redundant power supplies. [PT-5]<br><br>Physical and remote access to devices are secured and properly managed. [AC-1 through AC-4]<br><br>Protect PNT user equipment data. [DS-4] | 4, DS-6, DS-8] | compromise of the PNT data are *understood and communicated* before continuing operations.[ AN-2]<br><br>*Alert stakeholders* including the device manufacturer of hardware faults or failures describing the limitations and extent of disruption in PNT source integrity. [CO-2, CO-3] | 1]<br><br>*Update the recovery plan* to incorporate lessons learned, reflect new threats, improve technology, and address changes to the organization, PNT system, operating environment, and problems encountered during plan implementation, execution, and testing. [IM-2] |
| **Data in transit**: Includes intentional or unintentional sources of disruption and manipulation of PNT data or signal in transit. Examples of transmission threats include path delay variations, multipath interference, jamming, and spoofing. | *Identify vulnerabilities and threats* to the communication modes from external PNT sources and internal networks transmitting and receiving PNT data and signals. [RA-1, RA-3]<br><br>*Identify PNT signal and data communication threats.* Follow information sources from ISACs and bulletins such as NANUs, NOTAMs, Safety Information Bulletins (SIBs) to be aware of possible disruption of PNT sources in a given area and | *Consider multiple communication paths and complementary PNT sources.* A resilient communications network topology can limit the impact of communication attacks. [IP-9]<br><br>*Apply communication technologies* that preserves integrity and improves the reliability and resilience of the PNT information. [DS-2, PT-4, IP-2]<br><br>*Use latest software and firmware* after testing and | *Integrity monitoring.* Continuous monitoring of the PNT data in transit and control effectiveness. [CM-1]<br><br>*Event logging* including both normal and anomalous communication states. [AE-3]<br><br>PNT data *alert thresholds* are established. [AE-5] | Execute *contingency procedures* and assess functionality of systems relying on complementary PNT sources or alternative modes of PNT communications. Notify downstream users of potential PNT data availability and integrity impacts. Record new threats and vulnerabilities. [RP-1, MI-1, MI-2, MI-3]<br><br>Continue to *log data* from all PNT sources as | *Execute recovery plan.* Equipment with adaptive algorithms and networks can switch to use available communication channels with minimal PNT availability and integrity degradation. Verify backup PNT sources are serviceable, operational, and sufficient before continuing operations safely. [RP-1]<br><br>*Update risk assessment.* Improve PNT training, testing, monitoring, detection, response, |

| Example Scenarios | Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|---|
| | time frame. [RA2]<br><br>*Identify communication resilience capabilities.* Consider how other sensors can be leveraged to monitor and detect anomalies in PNT sources. [BE-5] | characterization. [MA-1]<br><br>*Calibration and characterization of PNT system uncertainty* including establishment of testing, certification, and continuous monitoring and integrity alert thresholds expectations under operational environmental conditions. [MA-1]<br><br>*Network integrity protection*. Provide capabilities to monitor and where feasible, segregate networks. [AC-5] | | feasible. [AN-1]<br><br>*Operational constraints* due to the loss of the PNT data are *understood and communicated* before continuing operations.[ AN-2]<br><br>*Alert user community* of communication disruptions describing the limitations and extent of disruption in PNT source *integrity and availability.* [CO-2, CO-3] | recovery procedures, and resiliency features. [IM-1]<br><br>*Update the recovery plan* to incorporate lessons learned, reflect new threats, improve technology, and address changes to the organization, PNT system, operating environment, and problems encountered during plan implementation, execution, and testing. [IM-2] |
| **Supply chain:**<br><br>Includes disruptions, degradations, or compromise of PNT services, software or hardware components, including counterfeiting, leading to components that may not be as reliable or components that have been maliciously | *Identify the role of the organization or critical infrastructure in providing PNT services.* Organizations using a PNT source to re-broadcast or transmit PNT data must be aware of how changes can impact PNT data and signals downstream. [BE-1, BE-2]<br><br>*Suppliers and third party testing and certification*. Identify relevant conformance testing and certification requirements | *Suppliers and third party partners understand their roles and responsibilities.* [AT-3]<br><br>*Hardware component authentication* such as radio-frequency identification (RFIDs), physically unclonable functions (PUFs), or other markers. [AC-1, AC-6, AC-7]<br><br>*Hardware lifecycle management* to include | *Clarify monitoring and detection responsibilities* and support open communication channels among supply chain to analyze and support root cause determination of anomalous PNT data or signal output. [AE-3]<br><br>*Understand risk impacts among supply chain partners*. Policies and procedures, including lessons learned over | Execute *contingency procedures* and assess functionality of systems relying on complementary PNT services or other third-party services. Notify downstream users of potential PNT data availability and integrity impacts. Record new threats and vulnerabilities. [RP-1, MI-1, MI-2, MI-3]<br><br>*Operational constraints* | *Execute recovery plan.* Equipment and applications can switch to use available services or components with minimum PNT availability and integrity degradation. *Verify backup PNT sources* are serviceable, operational, and sufficient before continuing operations safely. [RP-1]<br><br>*Update the recovery plan* to incorporate lessons learned, reflect new |

| Example Scenarios | Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|---|
| modified. | and processes. [SC-2]<br><br>*Identify vulnerabilities, including sources of errors, and threats* in the PNT supply chain. For example, when PNT services are transferred through multiple parties and locations. [RA-1, RA-3]<br><br>Assure *the total uncertainty* remains within industry standards and regulatory requirements. [GV-4] | proper disposal. [DS-3] | time, are adequately documented and shared with stakeholders. [AE-4]<br><br>PNT data *alert thresholds* are established. [AE-5]<br><br>*Verify PNT device integrity*. Identify and document known limitations. [DS-6, DS-8] | due to the loss or compromise of the PNT services or components are *understood and communicated* before continuing operations.[ AN-2]<br><br>*Alert user community* of supply chain disruptions and threats describing the limitations and extent of the threat in PNT source *integrity and availability.* [CO-2, CO-3] | threats, improve technology, and address changes to the organization, PNT system, operating environment, and problems encountered during plan implementation, execution, and testing. [IM-2] |

# Appendix E—Organization Specific PNT Profiles

NISTIR 8323 provides the foundational set of cybersecurity outcomes based on the five functions of the NIST Cybersecurity Framework relevant to the responsible use of PNT sources and data. The set of outcomes selected by the organization based on its mission and business objectives are intended to manage the risks associated with the use of PNT data. However, it should be noted that implementation of the foundational profile is necessary but not complete compliance with Executive Order 13905. This appendix will provide guidance to PNT stakeholders on applying the NISTIR 8323 to create sector-specific and organization PNT user profiles and to address other aspects of the Executive Order.

Creating a custom PNT profile based on the foundational profile is beneficial to an organization, especially if they are part of a critical infrastructure. Each custom PNT profile is intended to capture the requirements of an organizations PNT source and data and a prioritized set of PNT data security outcomes. The custom PNT profile can be used to inform new PNT source and services acquisitions process when researching and evaluating PNT services and sources. In accordance with EO 13905, the U.S. government will develop contractual language to include relevant cybersecurity outcomes from the foundational PNT profile as potential requirements in federal contracts for products, systems, and services that use or integrate PNT services. A custom profile will facilitate a systematic risk management process for the use of PNT data to meet sector-specific regulatory and standards requirements. In addition, an organizational PNT profile would enable assessment of their ability to satisfy the contract when using and providing PNT sources and data.

Organizations have different assets, architectures, cybersecurity resources and tolerances to PNT denial or disruption. Accurate, comprehensive, and systematic assessments regarding the responsible use of PNT requires knowledge of assets, any cybersecurity measures in place, knowledge of any external dependencies and the impact should there be a loss or degradation of PNT data that is in the context of the individual organization. Generating the assessment and definition of a way forward to achieve the appropriate level of PNT assurance will require leadership and a cadre of subject matter expertise such as:

- The Chief Information Officer (CIO). Manages people, processes, and technologies within the IT organization with the ability to influence the direction of resources for greater assurance or accept the residual risk.
- Cybersecurity Experts. Provides knowledge of cyber-threats and the ability of the current or proposed IT infrastructure's ability to mitigate attacks.
- Operators and Operations Management. Provides knowledge of daily operations and the impact of an incident or the impact of changes to the IT system on operations.
- Users of PNT Data. Provides insight on the impact should the organization's products or services be delayed, degraded or lost. Provides knowledge of PNT application uses cases and PNT data performance, reliability, and resilience measures.
- System Administration. Configure systems or gather information to provide data for engineering, analysis or enforce technical and managerial controls.
- IT and System Design. Provides knowledge of current or proposed designs and propose new or modified components or systems.

- System Engineering. Integrates modifications or designs of systems providing or transmitting PNT information.
- Marketing and Sales Personnel.

Aggregation or easy access to relevant information will expedite the PNT Profile development process for an organization. This is especially important for the Identify function and will aid in the ability to evaluate the degree of the organization's implementation of the categories and subcategories within all of the functions. The type of information that will be needed will include:

- Any standards, guides, policy, regulations, best practices, concept of operations, continuity plans, cybersecurity incident response and recovery plans, risk management documentation, and other documentation that applies to the organization's business and mission objectives.
- Network and system architecture and diagrams with details such as:
  - Boundaries
  - Interfaces
  - Information flows
  - Connectivity
  - Any external dependencies (especially PNT related dependencies)
- Network access points to include any temporary access points (such as wireless access points) or hardware interfaces (such as USB drives, CD's)
- Inventory of assets and their deployment.

Once the team is assembled and the background information is made available, a systematic analysis of the foundational profile can be made in the context of the individual organization. Some of the subcategories will require much more robust implementations (relative to other organizations) while other subcategories may not be as critical.

The organization will have applicable knowledge of their specific protection measures and the organization's personnel will provide information that is unique to the organization. As a part of its findings, the team can provide references, documentation, and other artifacts to supplement the informative references provided by the Foundational PNT profile. The findings of the team will enable executives and leaders to make informed decisions regarding the "As is" or "Proposed" PNT posture.

1735 This table contains changes that have been incorporated into NIST Interagency or Internal
1736 Report (NISTIR) 8323 revision 1. Change log updates can include corrections, clarifications, and
1737 or other major and minor changes in the publication that are either *editorial* or *substantive* in
1738 nature.

1739 **Table 26 - Change Log**

| Date | Type | Change | Pages |
|---|---|---|---|
| 6-01-2022 | Editorial | RTCA 229: Reference was misplaced, moved from ID.AM-1 to ID.BE-5 | 12, 21 |
| 6-01-2022 | Editorial | RCTA 292: Reference was misplaced, moved from ID.AM-1 to ID.RA-1 | 12, 24 |
| 6-01-2022 | Editorial | RCTA 326: This is an airworthiness specification. Does not apply to ID.AM-1. Deleted reference. | 12 |
| 6-01-2022 | Editorial | USG FRP: Reference was misplaced. Moved to ID.GV | 12, 22 |
| 6-01-2022 | Substantive | Added ID.BE-1 with informative references. Applicable to organizations that receive and rebroadcast PNT | 17 |
| 6-01-2022 | Substantive | Added ID.BE-2 and informative references. PNT supports and is impacted by other elements of the critical infrastructure | 18 |
| 6-01-2022 | Substantive | Added reference to ID.GV-4; UTC(USNO) and UTC(NIST) for data products on time difference between UTC(NIST) from UTC(USNO) | 22 |
| 6-01-2022 | Substantive | Added reference to ID.GV-4; Obtaining USNO data products to establish time differences between GPS and UTC(USNO) | 22 |
| 6-01-2022 | Editorial | Removed VIM reference in ID.GV-4. Is a general document about uncertainty | 22, 91 |

| Date | Type | Change | Pages |
|---|---|---|---|
| | | measurement, too generic for this document. | |
| 6-01-2022 | Editorial | Removed two references in ID.RA-1. Out of date threat documents. (1995 and 2001) | 24, 91 |
| 6-01-2022 | Editorial | Removed CSF references for any specific subcategory. The CSF applies equally to all the Subcategories | Multiple pages |
| 6-01-2022 | Substantive | Added the Risk Management Strategy category and added ID.RM-1 and ID.RM-3 Subcategories with informative references. | 30,31 |
| 6-01-2022 | Substantive | Added the Protect Awareness and Training category and added PT.AT-3 subcategory with informative references. | 40 |
| 6-01-2022 | Editorial | Added “residual risk” to the glossary | 112 |
| 6-01-2022 | Editorial | Removed NISTIR 8250 reference from PT.DS-8. Is a general reference for calibration procedures and does not apply to hardware integrity measures. | 46 |
| 6-01-2022 | Editorial | Removed IETF 7882 from reference section. Was not specifically referenced in any subcategory | 85 |
| 6-01-2022 | Editorial | Removed NISTIR 8250 from reference section. Was a general reference for calibration procedures | 88 |
| 6-01-2022 | Editorial | Updated NIST SP 800-160-2 reference to current version | 100 |
| 6-01-2022 | Editorial | Added “agility” to glossary | 106 |

| Date | Type | Change | Pages |
|---|---|---|---|
| 6-01-2022 | Substantive | Appendix D PNT User Risk Management | 139 |
| 6-01-2022 | Substantive | Appendix E Proposed Summary of CISA Language in a new appendix to include reference to contract language | 131 |
| 6-01-2022 | Substantive | Added reference [IEEE 1139] to ID.RA-4, PT.MA-1, PT.DS-6, and references section. | 27 |
| 6-01-2022 | Substantive | Added reference [IEEE 1193] to ID.RA-4, PT.MA-1, PT.DS-6, and references section. | 27 |
| 6-01-2022 | Substantive | Added reference [ISO 17025] to PT.DS-6 and to references section. | 44,45 |
| 6-01-2022 | Substantive | Added risk management and PNT references to Appendix D. | 122-129 |
| 06-03-2022 | Substantive | Added reference [3GPP TS 22.071] to ID.AM-5 and references section. | 15,16,88 |
| 06-03-2022 | Substantive | Added reference [FCC E911] to ID.GV-4 and references section. | 22,91 |
| 06-03-2022 | Editorial | Updated references [3GPP TS36.305], [3GPP TR22.826], [3GPP TR22.878], [DHS GPS CI], [DHS RCF], [DIA], [GPS], [GPS IS-200], [GPS IS-705], [GPS IS-800], [GPS ICD-240], [IEC 62439-3], [IEEE 802.1AS], [ITU-T G.8275.1], [NAVCEN], [NIST SP 800-161], [NISTIR 8320] to reflect the latest versions and links. | 88-103 |
| 06-03-2022 | Substantive | Added [IETF 5905] to references section. | 94 |
| 06-03-2022 | Substantive | Added reference [DHS S&T 2022] to ID.BE-1, ID.BE-2, PT.AT-3, and references section. | 17,18,40,90 |

| Date | Type | Change | Pages |
|---|---|---|---|
| 06-14-2022 | Substantive | Added references [GAL ICD] and [BDS ICD] to ID.AM-3, ID-GV.4, PT.DS-6, DE.AE-3, and references section. | 14,23,44, 62, 88, 91 |
| 06-14-2022 | Substantive | Added additional sensor controls to ID.AM-1, Acronyms, and Glossary sections. | 12,105 |
| 06-14-2022 | Substantive | Added geodetic accuracy of WGS84, performance expectations of GPS position and time accuracy, and reference [GPS SPS] for additional GPS performance expectations to ID.GV-4. | 22,23 |
| 06-14-2022 | Substantive | Added informative reference [NOAA SWS] to ID.RA-3. | 26, 101, 102 |
| 06-14-2022 | Substantive | Added informative reference [SPD-7] to DE.AE-3 to understand sector-specific agencies responsible for monitoring the civil performance of space-based PNT services. | 62, 103 |
| 06-14-2022 | Substantive | Added concept of resilience levels [DHS RCF] of the equipment as part of the PNT user system recovery plan [PT.IP-9] and process [RC.RP-1]. | 49,84 |
| **Date** | **Type** | **Change** | **Pages** |
| 10-16-2019 | Editorial | Fixed misspellings in Executive Summary. | vi |
| 10-16-2019 | Substantive | Replaced introductory paragraph in Section 2. | 12 |