NIST Internal Report
NIST IR 8323r2 pd

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

Public Draft

Joseph Brule
Nakia Grayson
Ya-Shian Li-Baboud
Suzanne Lightman

James McCarthy
Karri Meldorf
Doug Northrip
Arthur Scholz
Theresa Suloway

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8323r2

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8323r2 pd

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

Public Draft

Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Ya-Shian Li-Baboud
Applied and Computational Mathematics Division
Information Technology Laboratory

Nakia Grayson
James McCarthy*
Applied Cybersecurity Division
Information Technology Laboratory

Joseph Brule
Karri Meldorf
Doug Northrip
Arthur Scholz
Theresa Suloway
The MITRE Corporation

* Former NIST employee; all work for this publication was done while at NIST

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8323r2

May 2026

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Supersedes NIST IR 8323r1 (January 2023)

How to Cite this NIST Technical Series Publication:
Lightman S, Li-Baboud YS, McCarthy J, Brule J, Meldorf K, Northrip D, Scholz A, Suloway T, Grayson, N (2026) Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8323r2 Draft. https://doi.org/10.6028/NIST.IR.8323r2

Author ORCID iDs
Suzanne Lightman: 0000-0002-50007-3887
James McCarthy: 0000-0002-5559-733X
Ya-Shian Li-Baboud: 0000-0003-3234-4345
Nakia Grayson: 0000-0003-1062-4338
Joseph Brule: 0000-0002-7987-6050
Karri Meldorf: 0000-0003-3617-3846

Contact Information
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

Public Comment Period
May 6, 2026 – July 6, 2026

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

Abstract

The national and economic security of the United States (U.S.) is dependent upon the reliable operation and responsible use of Positioning, Navigation, and Timing (PNT) services. This document provides the Cybersecurity Framework (CSF) Version 2.0 Community Profile developed for supporting positioning, navigation, and timing (PNT) services 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.

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.

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

Table of Contents

184 ## List of Tables

206 ## List of Figures

Acknowledgments

The authors wish to thank all individuals and organizations, that provided contributions and comments in the creation of Revision 2 and prior versions of this document: Michael Striffolino, James Platt, Mary Beth Perry, Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA); Ernest Wong, DHS Science and Technology Directorate (S&T); Thelma Allen, Michael Bartok, Lisa Carnahan, Amber Crutchfield, Katya Delak, Elizabeth Donley, James Foti, Jonathan Hardis, Judah Levine, Michael Lombardi, Cherilyn Pascoe, Karen Reczek, Kristina Rigopoulos, Matthew Scholl, Kevin Stine, James St. Pierre, and Isabel Van Wyk, National Institute of Standards and Technology (NIST); Michael Calabro, Booz Allen Hamilton; Michael Lewis, Chevron; Justin Perkins, CTIA; Gerry Trevino, JBSA 5G Next Gen; Jion Kim, Hyundai America; Betsy Barron, Robin Drake, Jason Kuruvilla (former employee), Christina Sames, Lauren Swan, and Thomas Walters, MITRE; John Fischer, Orolia; Kenneth Sheperd, Peraton; Francisco Girela, Safran; David Howard, U.S. Department of Energy (DOE); Karen Van Dyke, U.S. Department of Transportation (DOT).

Executive Summary

The PNT Profile provides a flexible framework for users of PNT services to manage risks when forming or using PNT signals or data, which are susceptible to disruptions and manipulations that can be natural, manufactured, intentional, or unintentional. It was created by applying the NIST Cybersecurity Framework (CSF) version 2.0 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 by considering and adopting the recommendations in the Profile. Organizations can apply the PNT Profile within risk management programs to protect their systems and assets from the disruption or manipulation of PNT services and data. The Profile is intended to guide users in establishing responsible strategies for managing PNT cybersecurity risks.

The PNT Profile is voluntary and does not: constitute regulations, define mandatory practices, provide a checklist for compliance, or carry statutory authority. It is intended to be a foundational set of guidelines. Sector Risk Management Agencies (SRMAs) 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.

This revision updates the PNT Profile to align with the NIST CSF 2.0. CSF 2.0 can serve all organizations, regardless of sector or size, with the objective to provide accessible and actionable guidance for all users, including but not limited to critical infrastructures, private industry, and small businesses. Organizations can apply the profile to align their PNT use with their broader enterprise risk management strategy. Because PNT services can be critical to modern services and operations, key updates from the previous version include the integration of the CSF Govern Function, updates to Functions, and Categories to reflect the need for executive-level risk management strategies and oversight to achieve PNT resilience. PNT services often rely on external suppliers, such as the satellites' signals and the third-party manufacturers of receivers and antennas. CSF 2.0 elevates cybersecurity supply chain risk management in the Govern function. Updates to informative references have also been made throughout the document to reflect the latest guidance and risk mitigations.

1. Introduction

This PNT Profile revision is being issued to update the PNT Profile to conform with the NIST Cybersecurity Framework 2.0. The informative references have also been reviewed and updated.

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 could result from the disruption or manipulation of PNT data. The PNT Profile serves as a guide to risk-informed management of PNT services to enable operational resilience and minimize the impact of signal disruptions or manipulations on critical functions.

Use of the PNT Profile will help organizations:

- Establish governance mechanisms to address risks in the management and use of PNT services and data;
- 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;
- 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 was originally developed under Executive Order 13905 (EO 13905), *Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services*. 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 and United States Naval Observatory (USNO) 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 Fig. 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 national and economic security. In this case, responsible use by organizations includes incorporation of actionable goals, including but not limited to:

- Risk-informed management of systems' functions such that they remain operational or fail-safely when PNT signals are unavailable or compromised;
- Risk-based approaches that can detect degradation and alert applications when position and time data quality are compromised, and 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.

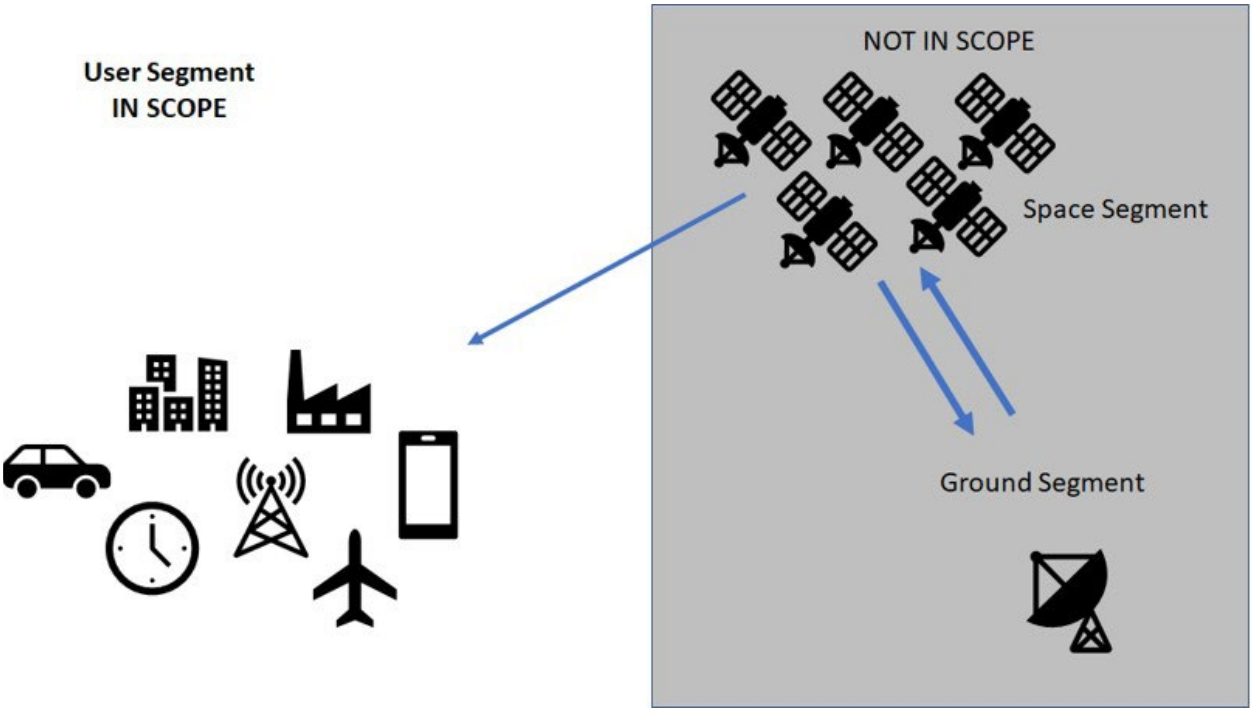


Fig. 1. Example of How the PNT Profile Applies to GNSS

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 guidance if more specific risk management efforts may be required. Organizations within various sectors can customize the PNT Profile by considering the following [NIST-CSF-OP]:

- What risk management governance strategy and outcomes need priority for PNT data and services?
- 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 inclusion in NIST CSF 2.0 of the Govern Function is to emphasize the importance of addressing cybersecurity risk within the context of business risk.

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 that can be used with the NIST CSF are included in Appendix A of the PNT Profile.

3.2. Cybersecurity Framework Overview

Created through collaboration between industry and government, the 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. Many organizations in the private and public sectors (including federal agencies) use the NIST CSF.

The NIST CSF consists of three main components:[1]

1. The *CSF Core* provides a catalog of desired cybersecurity activities and outcomes[2] using common language. The Core guides organizations in managing and reducing

[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".

their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.

2. The *CSF 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 *CSF Organizational 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 CSF Core presents standards, guidelines, and practices within six 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. **Govern:** Provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. The Govern Function addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.
2. **Identify:** Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under Govern. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.
3. **Protect:** Once assets and risks are identified and prioritized, Protect supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.
4. **Detect:** Detect enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.
5. **Respond:** Respond supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.

6. **Recover:** Recover supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

When considered together, these Functions provide a high-level, strategic view of an organization's PNT cybersecurity risk management life cycle. The CSF Core identifies underlying discrete cybersecurity outcomes (i.e., Categories and Subcategories) for each Function. The six Functions of the CSF 2.0 are composed of 22 Categories (e.g., "Asset Management" or "Data Security"), which are further broken down into Subcategories of more specific outcomes from technical and management activities. Table 1 shows the six Functions and 22 Categories of the Core.

Table 1. Cybersecurity Framework Functions and Categories

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

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

Function	Category	Subcategory		Informative References
Identify (ID)	**Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) 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-01	Inventories of hardware managed by the organization are maintained.	**NIST SP 800-53 Rev. 5** CM-8, CM-9 PM-5 **NIST SP 800-160 Rev. 1** 2, 3
		ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained.	**NIST SP 800-53 Rev. 5** CM-8, CM-9, CM-10, CM-11, CM-12, PM-5 **NTP-MON**

Fig. 2. Cybersecurity Framework Subcategory Example

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

The PNT Profile in Section 4 can be used as a foundation for organizations to tailor and develop their own custom Organizational Profile [NIST-CSF-OP], as shown in **Fig. 3**. Considering their unique PNT business and mission objectives, threat environment, and cybersecurity requirements, organizations can review the Subcategory guidance in the PNT Profile to determine which Subcategories to prioritize to meet the outcomes required by its governance structure: identification of systems dependent on PNT services, detect disruption and manipulation of PNT services, and manage the risks to those systems.

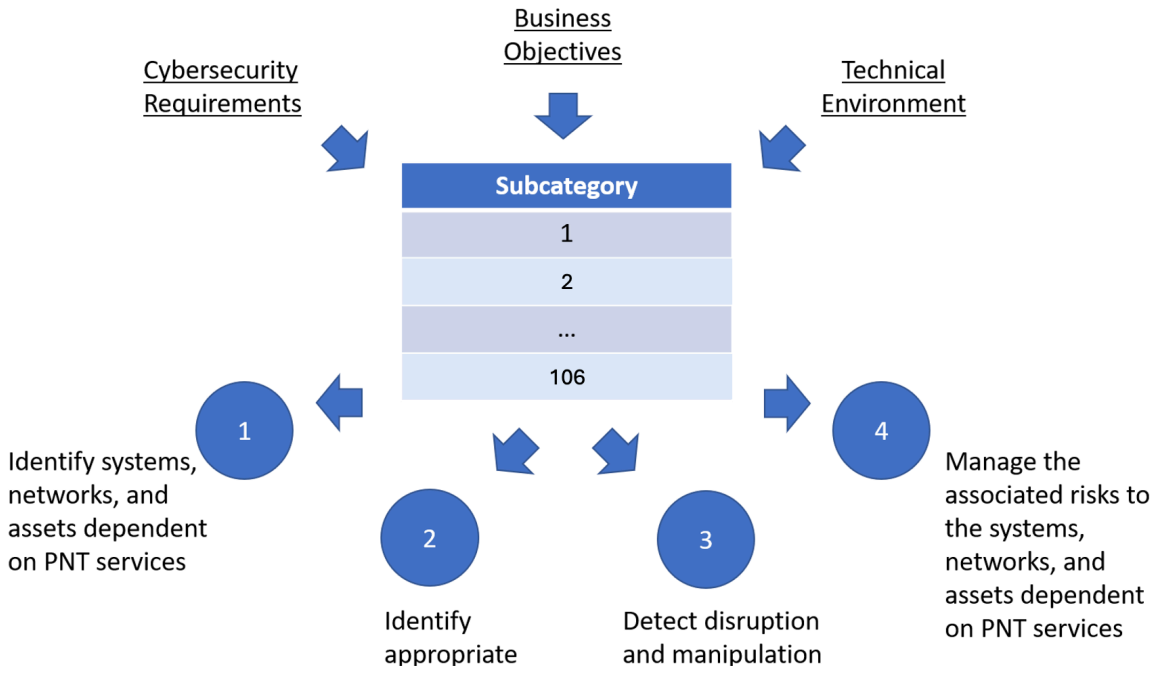


Fig. 3. Organizational PNT Profile Creation Process

The PNT Profile offers high-level cybersecurity risk mitigation strategies for PNT users, which can be tailored to an organization's PNT-specific business and regulatory needs. The PNT Profile can help organizations incorporate cybersecurity and can also be used to provide a baseline of PNT cybersecurity outcomes and activities for organizations within a sector or sub-

sector. A sector or sub-sector Profile can be further tailored or augmented to address a unique set of PNT cybersecurity requirements, business objectives, or threats.

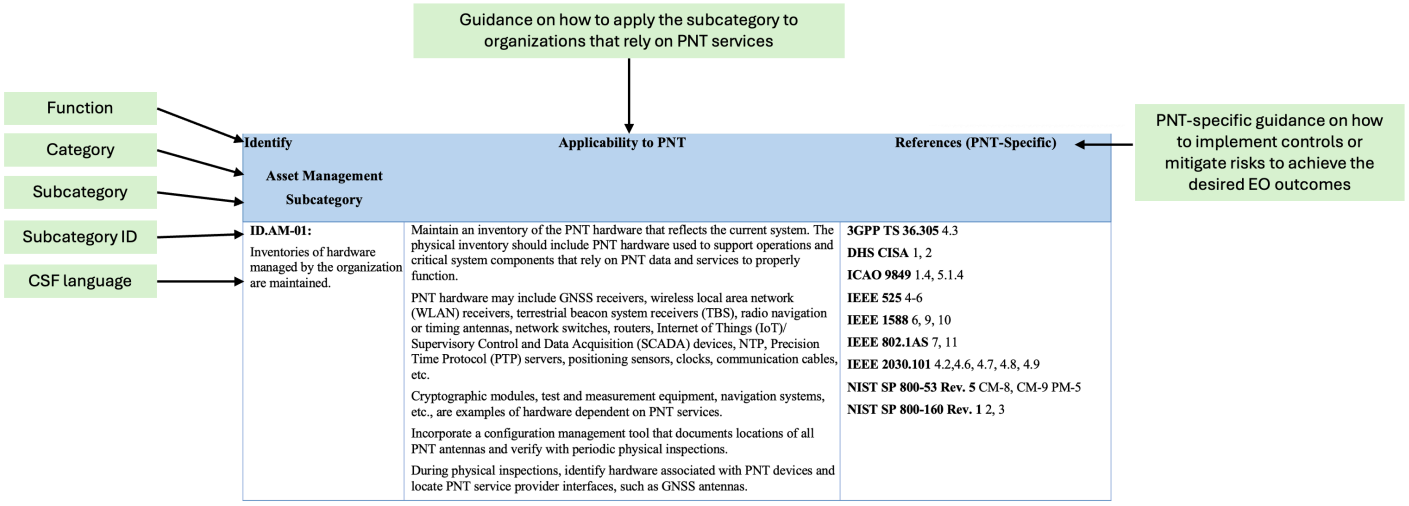
The PNT Profile is intended to be implemented within the larger context of an organization that is developing and executing its own cybersecurity program.[3] That program should be based on organizational cybersecurity risk management policies and procedures. This PNT Profile is best implemented if a 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.

4. The PNT Profile

This section was created by using the NIST CSF 2.0, as described in Sec. 3.2. Each table below in the PNT Profile summarizes the Subcategories for a specific Function and its Categories. The components of these PNT Profile tables are concisely summarized in **Fig. 4**. 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. Sections 4.1 through 4.6 provide insight into how the Subcategories address the responsible use of PNT. Note: Not all Subcategories in the NIST CSF 2.0 are listed here; only those most applicable to this PNT Profile are included. Acronyms described in the PNT Profile are listed in Appendix B.

Successful implementations require a comprehensive approach. The CSF Functions and guidance in the PNT Profile address the generic needs of PNT users that depend on PNT services to meet their business objectives. 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 or guidance defined in PNT references in Sec. 4.1 through Sec. 4.6.

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



495 **Fig. 4. Components of the PNT Profile**

4.1. Govern Function

The Govern Function covers how the organization's cybersecurity risk management strategy, expectations and policy are established, communicated and monitored. This Function provides guidance for how the other Functions should be applied. It specifically maps out the expectations of outcomes from the Profile process to the mission and stakeholders' expectations. The Govern Function is foundational to the successful application of a Profile.

The objectives of the Govern Function include:

- Specifying organizational context;
- Tying cybersecurity activities to organizational risk management strategies;
- Establishing roles, responsibilities, authorities and policies; and,
- Securing the cybersecurity supply chain.

The Govern Function within the NIST CSF defines six Categories. These Categories and their Subcategories are essential to a strong cybersecurity program. Within the context of the PNT Profile's scope (Section 1.2), four of Govern's Categories and subsets of each Category's Subcategories are specifically relevant to responsible use of PNT data.

4.1.1. Organizational Context (GV.OC)

Understand and assess circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions. Three GV.OC Subcategories, when the use of PNT data affects risk decisions within the Organizational Context, apply to the PNT Profile as summarized in Table 2.

Table 2. Govern – Organizational Context Subcategories Applicable to PNT

Govern Organizational Context Subcategory	Applicability to PNT	References (PNT-Specific)
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity – including privacy and civil	Be aware of legally accepted PNT standards and sources. For example, UTC(NIST) and UTC(USNO) are the sources of legal time in the U.S. Understand standards that support resiliency and interoperability for	**ACA 2007** 15 USC 205 **DHS-CISA-ACQ** **DHS S&T 2024** 3.1

Govern Organizational Context Subcategory	Applicability to PNT	References (PNT-Specific)
liberties obligations -- are understood and managed.	PNT services and national/international coordination to support the performance, standardization, and cost minimization of user equipment. 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. Specify and review contractual requirements for appropriate levels of resiliency based upon the operational needs of the proposed product, system, or service. Consider adaptability and flexibility in contractual clauses to address evolving, context-dependent risks.	**DOT-CPNT-AP** 2 **DOT-PNT-SP** **FAA 1770.68** **GPS-GNSS2** **IEEE 1952** **SAE J2945** 5,6 **NIST-SP-800-53 Rev. 5** PL1-PL7
GV.OC-04 Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	Critical objectives can include, but are not limited to, measurement uncertainty, continuity of operations, acceptable service downtime, drift, and stability tolerances. Cybersecurity capabilities include PNT threat awareness and detection. 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. For organizations that form PNT data, understand data provenance and integrity capabilities and limitations, service resilience levels, and customer dependencies on PNT data. Organizations supplying PNT services, including but not limited to re-broadcasting, need to assess the cascading effects that service interference may have on their users. Communicate to users and external stakeholders the critical PNT	**3GPP-TR-22.826** 5, 7.3 **3GPP-TS-22.104** 5, 7 **3GPP TS 22.261** 7.3 **DHS CISA** 2.b, 3.a, 3.b, 3.c **DHS RCF** 5 **DHS S&T 2022** **DHS S&T 2024** 3.1, 3.2 **ICAO 9613** 1, 3, 4 **NIST SP 800-53 Rev. 5** CP-2, PM-11, PM-31, PM-32, RA-9, SC-45, SI-1, SI-4, SI-5, SI-7, SI-10, SI-14, SR-3, SR-4, SR-9 **NIST TN 2189** II-VI

Govern Organizational Context Subcategory	Applicability to PNT	References (PNT-Specific)
	objectives, capabilities, service resiliency levels available.	**USG FRP** 4, 6
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated.	Identify and prioritize internal critical business services that are dependent on PNT system processes and components. Identify and prioritize supporting services for critical PNT system processes and components. The organization's infrastructure, such as network communication architectures and protocols, can impact recovery time in the event of a path or node failure. Communicate internally to information technology and security teams regarding the critical outcomes and capabilities of the PNT services available for PNT-dependent applications.	**DHS CISA** 1.a, 1.e **DHS RCF** 5 **FAA AIM** 1 **GPS** 2-13 **GPS SPS** 3 **IEEE 2030.101** 4.3-4.7 **NIST SP 800-53 Rev. 5** CP-1, CP-2, CP-8, PE-9, PE-11, PM-8, PM-16, RA-5, RA-7, RA-9, SA-17, SC-29, SC-38 **NIST TN 2189** II-VI

4.1.2. Risk Management Strategy (GV.RM)

The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions. Subcategories are relevant to the PNT Profile when the use or presence of PNT services or data affects the risk management strategy.

There are two GV.RM Subcategories that apply to the PNT Profile as summarized in Table 1.

521 **Table 3. Govern – Risk Management Applicable to PNT**

Govern Risk Management Strategy Subcategory	Applicability to PNT	References (PNT-Specific)
GV.RM-03 Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	Enterprise risk management requires a high-level understanding of how PNT data integrity impacts an organization's mission or business operations. Identify business processes that rely on PNT, which may include fleet logistics, timestamping transactions, and data center time synchronization. Understand the impact on business processes due to loss of PNT data availability. Develop a comprehensive strategy to manage risk to PNT-dependent operations. Include cybersecurity and risk-tolerance considerations. PNT cybersecurity outcomes include (1) PNT supply chain resilience through prioritized sources of component suppliers; (2) hardware, software, and data provenance; (3) signal monitoring and adversity detection; and (4) effective incidence response and recovery integration including graceful degradation or failover protocols. 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. 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 World Geodetic System 1984 (WGS 84) as the reference frame for positioning, and the GPS time scale is synchronized to UTC(USNO)	**DHS-CISA-ACQ** **DHS RCF** 5 **NIST SP 800-37 Rev. 2** 2, Annex D, E, F **NIST SP 800-53 Rev. 5** CP-1, CP-2, CP-8, PE-9, PE-11, PM-8, PM-9, PM-30, PS-1, RA-1, RA-3, RA-9, RA-10, SA-4

Govern Risk Management Strategy Subcategory	Applicability to PNT	References (PNT-Specific)
	within 1 μs.	
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.	Responsible use of PNT services includes the consideration of the acquisition, integration, deployment, operations, maintenance, repair, and replacement of PNT components and services. These considerations include the dependencies on the PNT primary sources and evaluation of the impacts as part of the PNT service acquisitions, systems integration, and deployment. The loss or degradation of an organization's capabilities or function may impact its customers, partners or other stakeholders. Consider and communicate the organization's risk tolerance to its stakeholders and its potential impact.	**DHS-CISA-ACQ** **NIST SP 800-53 Rev. 5** CP-1, CP-2, CP-8, PE-9, PE-11, PM-8, PM-16, RA-5, RA-7, RA-9, SA-17, SC-29, SC-38, SR-7, MA-1

4.1.3. Roles, Responsibilities and Authorities (GV.RR)

Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated. This Category is relevant when the use of PNT data or services impacts the assignment of such roles, responsibilities and authorities.

There is one GV.RR Subcategory that applies to the PNT Profile as summarized in the Table 4.

Table 4. Govern – Roles, Responsibilities and Authorities Subcategories Applicable to PNT

Govern Roles, Responsibilities and Authorities Subcategory	Applicability to PNT	References (PNT-Specific)
GV.RR-02:	When feasible, provision roles and responsibilities within a cooperative PNT risk management framework for data collection,	**ICAO 9849** 7.3, Appendix B

Govern Roles, Responsibilities and Authorities Subcategory	Applicability to PNT	References (PNT-Specific)
Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	data storage, and data dissemination towards improving future PNT protection, detection, response, and recovery capabilities. Understand PNT service provider and sector specific PNT risk management roles and responsibilities. Personnel understand routine responsibilities, such as patching receiver firmware and reviewing audit logs for anomalies, as well as incident response and recovery responsibilities such as execution of failover protocols.	**NIST SP 800-53 Rev. 5** CA-2, CA-7, IR-2, PL-2, PL-4, PM-10, PM- 14 **NIST SP 800-61 Rev. 3** 2.2 **NSM-22** **USG FRP** 2.1-2.4, 3.2.11

4.1.4. Supply Chain Risk Management (GV.SC)

Cybersecurity supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders. Subcategories under this category are relevant to the PNT profile when the use of PNT data or services impact the applicability of the category.

There are four GV.SC Subcategories that apply to the PNT Profile as summarized in Table 5.

Table 5. Govern – Supply Chain Risk Management Subcategories Applicable to PNT

Govern Supply Chain Risk Management Subcategory	Applicability to PNT	References (PNT-Specific)
GV.SC-03 Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise	Remain apprised of current and future supply chain threats and associated regulations related to the acquisition of PNT services, sources, and devices forming, transporting, or using PNT data. Likelihood determination of PNT supply chain exploits include (i)	**DHS ACQ** **FAA 1770.68** **NIST SP 800-53 Rev. 5** RA-3, SR-2,

Govern Supply Chain Risk Management Subcategory	Applicability to PNT	References (PNT-Specific)
risk management, risk assessment, and improvement processes.	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.	SR-3, SR-5 **NIST SP 800-161** 2, Appendix A
GV.SC-04 Suppliers are known and prioritized by criticality.	Identify any external systems or services that the organization uses for ingesting PNT data or is dependent on for its PNT data. Mission criticality of PNT systems and components, along with impact analysis of supply chain vulnerabilities, threats, and likelihood can be used to determine the organization's risk and guide the selection of supply chain security controls.	**DHS GPS CI** A.2 **GPS-GNSS** **GPS-GNSS2** **GPS-SPS** **NIST SP 800-53 Rev. 5** SR-4, SR-6 **NIST SP 800-161** 3
GV.SC-06 Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships. PNT cybersecurity requirements are explicitly integrated into supplier contracts.	Consider verification and validation of PNT data and services when integrating third party systems or services. Technology control plans are established for acquiring and securing third party PNT equipment. *THIS IS BEING HELD FOR DISCUSSION WITH SMALL GROUP AND PUBLIC COMMENT*	**DHS ACQ** **FAA 1770.68** **NIST-SP-800-53 Rev. 5** PL1, PL7
GV.SC-07 The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the	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, risks, and risk tolerance; and (vii) the business objectives.	**DHS GPS CI** A.2 **FAR 52.204** 24 **NDAA 889** **NIST SP 800-37** 2.8 **NIST SP 800-161** 2.2

Govern Supply Chain Risk Management Subcategory	Applicability to PNT	References (PNT-Specific)
course of the relationship.	Supply chain vulnerabilities include (i) software systems and hardware 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. 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. PNT cybersecurity requirements are explicitly integrated into supplier contracts.	**NIST SP 800-53 Rev. 5** PM-9, RA-3, SR-2, SR-3, SR-5 **USG FRP** 1.7

4.2. Identify Function

The Identify Function provides guidance to support organizations in understanding their current PNT dependencies and associated cybersecurity risks. This understanding enables an organization to prioritize its effort to be consistent with its risk management strategy and the mission needs identified under the Govern Function.

The objectives of the Identify Function include:

- Identify the business or operational environment and organization's assets, including assets 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.

543 The Identify Function within the NIST Cybersecurity Framework defines three Categories, all of which have Subcategories that apply
544 to the PNT Profile, as summarized in Sec. 4.2.1 through Sec. 4.2.3.

545 4.2.1. Asset Management (ID.AM)

546 The assets (data, hardware, software, systems, facilities services and people) that enable the organization to achieve its business
547 purposes are identified and managed in a manner that is consistent with their relative importance to organizational objectives and the
548 organization's risk strategy. In the context of the PNT Profile, the assets that require and support PNT services in order to fulfill the
549 organization's mission and business objectives are identified.

550 There are six ID.AM Subcategories that apply to the PNT Profile, as summarized in Table 6.

551 **Table 6. Identify – Asset Management Subcategories Applicable to PNT**

Identify Asset Management Subcategory	Applicability to PNT	References (PNT-Specific)
ID.AM-01: Inventories of hardware managed by the organization are maintained.	Maintain an inventory of the PNT hardware that reflects the current system. The physical inventory should include PNT hardware used to support operations and critical system components that rely on PNT data and services to properly function. PNT hardware may include GNSS receivers, wireless local area network (WLAN) receivers, terrestrial beacon system receivers (TBS), radio navigation or timing antennas, network switches, routers, Internet of Things (IoT)/ Supervisory Control and Data Acquisition (SCADA) devices, NTP, Precision Time Protocol (PTP) servers, positioning sensors, clocks, communication cables, etc. Cryptographic modules, test and measurement equipment, navigation systems, etc., are examples of hardware dependent on PNT services. Incorporate a configuration management tool that documents locations of all PNT antennas and verify with periodic physical inspections. During physical inspections, identify hardware associated with PNT devices and	**3GPP TS 36.305** 4.3 **DHS CISA** 1, 2 **ICAO 9849** 1.4, 5.1.4 **IEEE 525** 4-6 **IEEE 1588** 6, 9, 10 **IEEE 802.1AS** 7, 11 **IEEE 2030.101** 4.2,4.6, 4.7, 4.8, 4.9 **NIST SP 800-53 Rev. 5** CM-8, CM-9 PM-5 **NIST SP 800-160 Rev. 1** 2, 3

Identify **Asset Management** **Subcategory**	**Applicability to PNT**	**References (PNT-Specific)**
	locate PNT service provider interfaces, such as GNSS antennas.	
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	The inventory should include PNT software, services and systems used to support operations and critical applications that rely on PNT data to properly function. Maintain an inventory of PNT software, services, and systems, such as software license information, software version numbers, human-machine interface (HMI), and other industrial control systems (ICS) component applications, and operating systems. Inventory of software, services and systems is reviewed and updated as defined by the organization. Identify all software, services, and systems that are dependent on PNT data, including hosts and applications relying on distributed time, using phase, frequency, and time 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 clock signals (e.g., 10 MHz, 1 PPS, and Inter-range instrumentation group time codes (e.g., IRIG-B, IRIG-J)). Software, services, and systems dependent on PNT data may include test and measurement tools, kernels, databases, logging software, cryptography/certificate management, and other applications that 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.	**3GPP TS** 36.305 4.3 **DHS CISA** 1.a, 1.b, 1.c, 2.a **DHS PNT** Appendix C **FINRA 4590** **FINRA 6800** **ICAO 9849** 1.4 **IEEE 1588** 5-14, Annex A, P **IEEE 802.1AS** 7, 10 **IEEE 2030.101** 4.3, 4.6 **IETF 5905** 5, 14 **ITU-T G.8261** 6, 7, Annex A **NIST SP 800-53 Rev. 5** CM-8, CM-9, CM-10, CM-11, CM-12, PM-5 **NTP-MON**
ID.AM-03: Representations of the organization's authorized	Identify and catalogue all dataflows within the PNT system, as well as between the PNT system and other systems. All connections and signal interfaces are documented, authorized, and reviewed.	**DHS CISA** 1, 2, 3 **DOT-PNT-SP**

Identify **Asset Management** **Subcategory**	**Applicability to PNT**	**References (PNT-Specific)**
network communication and internal and external network data flows are maintained.	Data flow 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. The ability to adapt interface availability and data flows in real-time can prevent further degradation. Identify the PNT data source and distribution medium for the applications and systems that meet 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. For each software that provisions or uses PNT data, identify the input and output data interfaces. Examples of external systems include engineering design services and those that are controlled under separate authority, personal devices, and other hosted services.	**GAL ICD** **GPS SPS** B.1.2, B.1.3, 14 **ICAO-9613** 3 **IEEE 802.1AS** 7.4, 8.5 **IEEE 1588** 8-12 **IEEE 2030.101** 4.2-4.11 **IEC 61850-90-4** 10 **IETF 5905** 5-14 **IETF 7384** 5, 7 **IMO 1575** A-D, Appendix C **IS-GPS-200** 3 **IS-GPS-705** 3 **IS-GPS-800** 3 **ITU-T G.8261** 6 **ITU-T G.8262** 6-12, Appendix III **ITU-T G.8272** 6-9 **NIST SP 800-53 Rev. 5** AC-4, CA-3, CA- 9, PL-8, SA-17 **RTCA 326** 3.1.1 **SAE J3161** 5
ID.AM-04:	Identify and maintain an inventory of all services provided by PNT sources. This inventory should include all sources as well as external connections used by the	**DHS CISA** 1, 2

Identify **Asset Management Subcategory**	**Applicability to PNT**	**References (PNT-Specific)**
Inventories of services provided by suppliers are maintained.	organization for PNT data. Suppliers could provide services controlled under separate authority and based on external systems, such as the cloud.	**GPS USER** **NIST SP 800-53 Rev. 5** AC-20, PM-5, SA- 9 **USG FRP** Appendix B
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.	As part of the prioritization of PNT assets, determine required resources to support current regulations and standards requirements for the responsible use of PNT systems. Assign adequate staff such that PNT support is available in timely manner, commensurate with thresholds defined in the organization's risk management process. Formalize PNT roles and provide a process for transitioning personnel to be replaced. Identify and prioritize PNT system components, processors, functions, and data based on their classification, criticality, and business value. Identify and prioritize the types of information related to PNT in the organization's possession, custody, or control for which security safeguards are needed (e.g., sensitive or protected information). 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. When identifying resources and prioritizing trade-offs for PNT systems, holistically consider requirements, such as availability, continuity, data integrity, timeliness of anomaly detection, response, and recovery.	**3GPP TS22.071** 4 **3GPP TS23.271** 4 **DHS CISA** 3 **ISO 15939**: 6.3.2.3 **NIST SP 800-37** 3 **NIST SP 800-53 Rev. 5** AC-20, RA-9 **USG FRP** Appendix B
ID.AM-07: Inventories of data and corresponding metadata for designated data types are	Identify, categorize, and maintain an inventory of all PNT data, metadata and all data that pertain to an event or the status of the PNT source. Types of PNT data and corresponding metadata include observation, navigation, timing, and correction data. Metadata and related standards to consider include	**ASPN 2023** **IGS RINEX** **NMEA 0183**

Identify **Asset Management** **Subcategory**	**Applicability to PNT**	**References (PNT-Specific)**
maintained.	Receiver Independent Exchange Format (RINEX), NMEA, and all-source PNT network (ASPN). Event or status data include real-time indicators and logs. Examples of such data include system integrity and health status, signal power levels, and error residuals. For timing, status data can include synchronization state, primary time reference, leap second status, or holdover status. Such data can indicate how well the system is performing and whether anomalous conditions exist. Logs can include epoch timestamps, source ID, event code, and configuration snapshots can be useful in tracing PNT service faults. 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. Some of the PNT data 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.	**NIST SP 800-53 Rev. 5** AU-8, RA-2, CM-8, MP-6, PE-16, PE-20

4.2.2. Risk Assessment (ID.RA)

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 eight ID.RA Subcategories that apply to the PNT Profile, as summarized in Table 7.

Table 7. Identify - Risk Assessment Subcategories Applicable to PNT

Identify Risk Assessment Subcategory	Applicability to PNT	References (PNT-Specific)
ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.	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. 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. 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. Vulnerabilities for an operational environment may include the susceptibility to atmospheric and scintillation effects on PNT signals, spoofing unauthenticated signals, or disruptions or manipulations of PNT services. Conduct vulnerability scans on PNT systems where safe, feasible, and in a manner that is consistent with industry best	**DHS CISA** 1.a, 4.a **DHS GPS CI** **ICAO 9849** 5, 7.13 **IEEE 2030.101** 4.12, 4.14, 5 **NIST SP 800-115** 2-8 **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 **NTP SEC** **RTCA 229** 1.6.2, 1.7.2, 2, 2.1.1.1.4, 2.1.1.1.5, 2.4, 2.5 **RTCA 356** 3.8.1, 3.8.2 **USG FRP** 1.7.3

Identify Risk Assessment Subcategory	Applicability to PNT	References (PNT-Specific)
	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.	

Identify **Risk Assessment** **Subcategory**	**Applicability to PNT**	**References (PNT-Specific)**
ID.RA-02: 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. 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. 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** **DHS CISA** 4.a **NCAS** **NERC EISAC** **NTP SEC** **NIST SP 800-53 Rev. 5** PM-15, PM-16 **USG FRP** Appendix B

Identify Risk Assessment Subcategory	Applicability to PNT	References (PNT-Specific)
ID.RA-03: Internal and external threats to the organization are identified and recorded.	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. 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.	**DHS CISA IE** **DHS GPS CI** **DHS RFI** **DIA** **DOT 12464** **GPS SPS** A.5.4.1 **ICAO 9849** 5, Appendix F **IETF 7384** 3 **IETF 9327** 6 **ITU-T 810** 6 **ITU-T GNSS** Appendix II, V, VII **Kaplan** 9, 10 **NASIC** **NIST SP 800-37** 2 **NIST SP 800-53 Rev. 5** PM-12, PM16, RA- 3, SI-5 **NIST SP 800-160 Rev. 1** 2.3 **NOAA SWS** **RTCA 235** 4-12 **RTCA 292** 2-14 **RTCA 326** 3.2 **RTCA 356** 3.2, 3.3, 3.4, 3.5

Identify **Risk Assessment** **Subcategory**	**Applicability to PNT**	**References (PNT-Specific)**
ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	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 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. Identify the potential business impacts of PNT service disruptions. The impact of a realized threat on PNT data performance 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 duration of the threat. 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. 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 PNT data error sources. Documenting PNT measurement uncertainty characteristics in conjunction with the assessed vulnerability exploits is useful to assess whether the PNT data meets mission requirements. For example, time signals and data are subject to phase variations due to frequency drift, 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.	**DOT 12464** **IATA RFI** **IEEE 1139** **IEEE 1193** **NIST SP 1065** 3-12 **NIST SP 800-53 Rev. 5** CP-2, PM9, PM-11, PM-9, RA-2, RA-3, RA-9 **NIST TN 1366** **RTCA 235** 2.1,13 **RTCA 236** **RTCA 292** 2.3-2.6

Identify Risk Assessment Subcategory	Applicability to PNT	References (PNT-Specific)
ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	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. 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. 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. 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. 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.	**5GAA-T4CAV** 4 **DHS GPS CI** **ICAO 9849** 5, Appendix F **IETF 7384** 3.1-3.3 **IETF 8633** 3-9 **IETF 8915** 3-9 **IETF 9327** **NIST SP 800-53 Rev. 5** CA-2, CA-7, PM- 16, PM-28, RA-2 **NIST SP 800-160 Rev. 1** 2.3, 2.4 **RTCA 235** 2.1-2.4, 3, 14 **RTCA 326** 2.1, 2.2, 3.1- 3.4 **RTCA 356** 2.7, 3.5
ID.RA-06 Risk responses are chosen, prioritized, planned, tracked and communicated.	For systems dependent on PNT data, risks include, but are not limited to (1) absence of PNT data; and (2) inaccurate or corrupted PNT data. Responses can be prioritized, planned, and adapted based on (1) effectiveness in limiting PNT data loss; (2) potential direct, residual, and side effects; and (3) multiple options if a selected	**DHS RCF** **DHS S&T 2025** 3 **NIST SP 800-160 Rev. 1** 2.3, 2.41 3.2, 3.5, Appendix E

Identify Risk Assessment Subcategory	Applicability to PNT	References (PNT-Specific)
	response does not achieve an intended result. Monitor and track the effectiveness and effects of selected risk responses. Planned risk responses should be communicated to relevant stakeholders including personnel, customers and other third parties as appropriate.	
ID.RA-08 Processes for receiving, analyzing, and responding to vulnerability disclosures are established.	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. Reference available public and private trusted sources of threat and vulnerability intelligence information as it relates to PNT.	**DHS RCF** 7, 8 **DOT 12464** **GPS-ICD-240** **ICAO 9849** 7.3 **NCAS** **NIST SP 800-53 Rev. 5** CA-1, CA-2, PM-4, PM-15, RA-1, RA-7, SI-5, SR-6 **NIST SP 800-61 Rev. 3** 3, 3.2 **NIST SP 800-160 Rev. 1** 3.4.9, 3.4.11 **NTP SEC** **RTCA 326** 3.4.4 **RTCA 356** 3.8 **USG FRP** Appendix B
ID.RA-10 Critical suppliers are assessed prior to acquisition.	PNT hardware and systems typically rely on multiple suppliers. For critical PNT services and data, consider current regulations and recording provenance.	**FAR 52.204** 24 **NDAA 889**

4.2.3. Improvement (ID.IM)

Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions.

There are four ID.IM Subcategories that apply to the PNT Profile, as summarized in Table 8.

Table 8. Identify – Improvement Subcategories Applicable to PNT

Identify Improvement Subcategory	Applicability to PNT	References (PNT Specific)
ID.IM-01 Improvements are identified from evaluations.	Characterize nominal and anomalous PNT data from tests for improving future monitoring and detection algorithms and resiliency capabilities. 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.	**DHS Integrity** **DHS RCF** 8 **IEEE 1952** **NIST-SP-800-53 Rev. 5** IR-3, SA-15
ID.IM-02 Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.	Validate that event detection processes are operating as intended. PNT device and component upgrades are re-validated with user end-to-end testing. Perform periodic testing to verify the performance of detection processes against the most current threat profiles and vulnerabilities. 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. 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.	**DHS RCF** 6 **DHS S&T** **ICAO 9849** 6 **IEC 61850-90-4** 14.2.4, 18 **IEEE 1952** **IEEE 2030.101** 5 **ITU-T GNSS** Appendix VII **NERC GridEx** **NIST SP 800-53 Rev. 5** CA-2, CA-7. PM- 14, SI-3, SI-4, CP-4, IR-3 **RTCA 229** 1.7.2, 1.7.3, 1.8.2.3, 2 **RTCA 326** 3.4.2, 3.4.4

Identify Improvement Subcategory	Applicability to PNT	References (PNT Specific)
	Consider the creation and maintenance of developmental and operational test and evaluation methods to assess, verify, and validate PNT service performance under normal and contested conditions.	
ID.IM-03 Improvements are identified from execution of operational processes, procedures and activities.	When practical, comply with standard data and message formatting, and message transmission to facilitate interoperability and integration. Modify and improve the monitoring strategy as new fault modes are identified and until detection performance is acceptable. Periodically examine the organization's PNT anomaly detection processes and seek to improve them continuously. Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned. Determine preventative actions for fault modes by reviewing the identification, protection, and detection Functions and updating as applicable. Revise protection, monitoring, detection, response, and recovery capabilities as needed to mitigate newly identified vulnerabilities in a timely manner. 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. Update risk assessments (refer to ID.RA-01) with newly identified PNT vulnerabilities, which are mitigated or documented as acceptable risks. PNT recovery plans incorporate lessons learned from ongoing incident handling activities into incident recovery procedures, training, and testing and implement the resulting changes accordingly.	**DHS CISA** 1.d **GPS ICD-870** 3.1 **ICAO 9849** 6 **IANA TZDB** **IEEE 1588** Annex J **IETF 9327** **IMO 1575** D, D.1, D.2, E.1 **NIST ITS** **NIST SP 800-53 Rev. 5** AC-4, CA-2, CA-3, CA-5, CA-7, CM-2, SC-16, PL-2, PM-14, RA-3, CP-2, IR-4, IR-8, RA-5, SI-4 **NIST SP 800-61 Rev. 3** 3 **NTP SEC** **RTCA 229** 1.5.2, 1.7.2 **RTCA 235** 14.1.4, 14.2-14.4 **RTCA 326** 3.4.1 **RTCA 356** 3.8 **USG FRP** Appendix B
ID.IM-04	Develop and maintain response and recovery plans that identify essential functions and associated contingency requirements, as well as provide a	**DHS RCF** 5, 6, 8

Identify Improvement Subcategory	Applicability to PNT	References (PNT Specific)
Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.	roadmap for implementing incident response. Plans should incorporate recovery objectives, restoration priorities, tests, metrics, contingency roles, personnel assignments, and contact information. Prioritize maintaining essential functions despite system disruption or manipulation, as well as the eventual restoration of the PNT devices and components. Communicate recovery activities to all relevant internal and external stakeholders, executive teams, and management teams. 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. Response planning can consider appropriate restrictions on the downstream consumption of PNT information to limit the impact of PNT disruptions. 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. 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	**DHS S&T** **DHS S&T 2022** 5 **DOT 12464** **ICAO 9849** 7.4-7.7 **IEEE 1952** 5.5, 5.6 **IEEE 2030.101** 5.4.2.5 **IMO 1575** C.2.1, C.2.2 **ITU-T GNSS** Appendix VII.3, VII.4 **NIST SP 800-34 Rev. 1** **NIST SP 800-53 Rev. 5** CP-2, CP-4, CP-10, IR-3, IR-4, IR-8, PM-14 **NIST SP-800-61 Rev. 3** **NIST SP 800-184** **NTP SEC** **RTCA 229** 2 **RTCA 326** 3.4.2, 3.4.4

Identify Improvement Subcategory	Applicability to PNT	References (PNT Specific)
	complementary PNT sources with multiple phenomenologies and an understanding of the benefits, limitations, and dissimilar failure modes to improve the PNT service's ability to detect anomalous inputs and remain available in contested environments. 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. Assess threat preparedness by verifying incident response and recovery plans of the PNT systems. 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. Results can inform detection algorithm improvement. 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. Testing response and recovery plans may include the use of RF signals to simulate anomalous events. Any simulation that involves RF transmissions must be conducted in a manner that is consistent with industry best practices and in accordance with laws and regulations. PNT response plans incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing	

Identify Improvement Subcategory	Applicability to PNT	References (PNT Specific)
	and implement the resulting changes accordingly. 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.	

4.3. 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 detected cybersecurity events with planning and preparation activities, while 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 five categories, all of which have at least one Subcategory that applies to this PNT Profile in varying degrees, as summarized in Sec. 4.3.1 through Sec. 4.3.5.

4.3.1. Identity Management, Authentication and Access Control (PR.AA)

Limit physical and logical access to PNT assets to authorized users and processes, consistent with the assessed risk of unauthorized activities. Assets may include antennas, receivers, servers, and subscriptions. Physical access includes facilities with PNT assets.

There are five PR.AA Subcategories apply to this PNT Profile, as summarized in Table 9.

Table 9. Protect - Access Control Categories Applicable to PNT

Protect Access Control Subcategory	Applicability to PNT	References (PNT-Specific)
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization.	Where applicable, establish and manage identification and authentication credentials of PNT users, data sources, and applications that use PNT data. 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. Revoke credentials when the authorization of PNT sources, devices, users, and processes expires or is no longer needed.	**DHS GPS CI** **IEEE 1588** Annex P 2.1.2 **IETF 5906** 7, 8, 10 **IETF 7384** 5.1 **IETF 8915** 1, 5.2, 5.6, 5.7, 8 **NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-10, IA-11, IA-12
PR.AA-02: Identities are proofed and bound to credentials based on the context of 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 time, geographical parameters, and environmental factors. Clients, applications, and systems are proofed for the authorized use and maintenance of PNT data or services.	**ATIS-I-0000070** 2-7 **IEEE 1588** 16.14, Annex P **IETF 4082** 2-5 **IETF 5906** 7, 8-10 **NISTIR 8014** 2-4 **NIST SP 800-53 Rev. 5** AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA- 5, IA-8, IA-12, PE-2, PS-3

Protect Access Control Subcategory	Applicability to PNT	References (PNT-Specific)
PR.AA-03: Users, services, and hardware are authenticated.	Implement source, client, or mutual authentication based on the information assurance requirements of the organization and be cognizant of how different applications may have different authentication requirements. Consider authenticating users, devices, and other assets for remote connections to the PNT data source. PNT data sources are validated for authenticity.PNT authentication strategies can be categorized by service-level (signal) and equipment-level (receiver, network). Service-level mitigations include use of authenticated signals and messages. PNT authentication mitigates risks associated with downstream operations, which depend on accurate and reliable PNT data. Authentication protects data provenance and verifies the authenticity of the data source. Understand that implementations may influence message delay and delay variations. Verify PNT data remains within tolerances. Timed Efficient Stream Loss-tolerant Authentication (TESLA) is a lightweight cryptographic protocol for PNT data verification. Not all PNT services support authentication, and alternatives should be sought when practical and warranted. At the equipment level, receivers can verify authenticity using PNT data consistency checks or signal filtering, such as antenna null-steering using controlled reception pattern antennas (CRPA).	**DHS CISA** 2.d, 5.b **DHS GPS CI** **GSC OSNMA** **IEEE 1588** 16.14, Appendix P **IETF 4082** 2-5 **IETF 5906** 2-12 **IETF 7384** 5.1, 5.7 **IETF 7822** 2-4 **IETF 8573** 3-7 **IETF 8633** 5.5, 5.6 **IETF 8915** 1,4, 5.5, 8.3, 8.4 **IS-AGT-100** 3, Appendix **NISTIR 8014** 4-6 **NIST-SP-800-61** **NIST SP 800-53 Rev. 5** AC-14, AC-17, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11, MA-4
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of	Create access control lists that enforce which authenticated users are authorized to use or perform actions on PNT systems. Enable approved access lists for all controls that follow, such as NTP and PTP time servers, signaling channels, and other PNT systems.	**IEEE 1588** Annex P 2.1.2, 2.5.2, 2.5.5 **IETF 8633** 3.4, 5.1 **NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC5, AC-6, AC-14, AC-16, AC-24

Protect Access Control Subcategory	Applicability to PNT	References (PNT-Specific)
least privilege and separation of duties.	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 authentication (e.g., during emergencies). Access controls are reviewed and updated throughout the systems, software, and service lifecycle.	**NIST SP 800-160 Rev. 1** Appendix F.1.14
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk.	Protect physical access to the PNT equipment, resources, and critical assets. Determine PNT data leak risks and mitigations. Determine access requirements during emergency situations. Maintain and review visitor access records to the facility where the PNT equipment resides, including antennas. 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** **NIST SP 800-53 Rev. 5** AC-5, AC-6, PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9, PS-3, PS-6, SC-26

4.3.2. Awareness and Training (PR.AT)

The organization's personnel are provided cybersecurity awareness education and training 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 is one PR.AT Subcategory that applies to the PNT Profile, as summarized in Table 10.

Table 10. Protect - Awareness and Training Subcategory Applicable to PNT

Protect Awareness and Training Subcategory	Applicability to PNT	References (PNT-Specific)
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind.	Adequate staffing with the appropriate training such that PNT support is available in a timely manner in accordance with thresholds defined in the organization's cybersecurity risk management plan. Formalize PNT roles and 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. 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, both initially and on an ongoing basis. 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. Appropriate training is provided to support current knowledge, maintenance, and use of PNT systems, hardware, software, services, and data. Operators, network and system administrators, and other technical staff are trained to install, test, and maintain PNT systems, as well	**DHS CISA** 1.f, 5.a, 7.a **DHS S&T 2022** **DHS RCF** 5.2, 8.3 **ICAO 9849** 1.3.1, 1.3.4, 7.3, 7.4, 7.5, 7.6.1 **IMO 1575** C.2.2 **ISO 27001** **NIST SP 800-34 Rev.1** 3.5, Appendix D **NIST SP 800-53 Rev. 5** AT-3, CP-2, CP-3, IR-3, IR-8, PS-7, SA-9, SA-16, PM-13 **NIST SP 800-160** Appendix E **USG FRP** 1.7.8, 5.1.2.5

Protect Awareness and Training Subcategory	Applicability to PNT	References (PNT-Specific)
	as to detect and respond to compromised PNT data with respect to the PNT data source and applications or systems that use PNT data. Ensure 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. Infrequent events, such as leap seconds, may be handled differently by different sources of PNT. Understand how these events and their implementations impact operations.	

4.3.3. Data Security (PR.DS)

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 three PR.DS Subcategories that apply to the PNT Profile, as summarized in Table 11.

600 **Table 11. Protect - Data Security Subcategories Applicable to PNT**

Protect Data Security Subcategory	Applicability to PNT	References (PNT-Specific)
PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are 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. 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. The sensitivity (confidentiality requirements) of PNT data may be impacted when bound or associated with other data.	**3GPP-TR23.271** 4.3 **GPS ICD-870** 3.3, 3.3.1 **IETF 9327** 6 **NIST SP 800-37** 3 **NIST SP 800-53 Rev. 5** MP-3, MP-4, MP-6, SC-28
PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.	Protect the PNT system against data leaks including network protocols and electromagnetic signal emissions. Special attention must be paid to PNT data which is bound to or used in conjunction with potentially sensitive data, such as PII. Use access control, 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. Consider using secure PNT data transmission protocols with multiple, complementary communication channels. Implement methods to verify integrity in the event of PNT data discrepancies among PNT sources. Some measures need to be considered at the architectural phase of	**3GPP-TR23.271** 4 **3GPP TS36.305** 4.3 **DHS CISA** 2.c **DHS GPS CI** 3 **DHS RCF** 5.2, 7, 8 **DHS S&T** **GAL ICD** **GPS GNSS** **GPS GNSS2** **ICAO 9849** 2.2.2, 4.1-4.4, 7.8, 7.10 **ICD-GPS-240** **ICD-GPS-870**

Protect Data Security Subcategory	Applicability to PNT	References (PNT-Specific)
	the SDLC, such as transport security implementations, while others can be applied at the configuration or deployment phase. For example, some NTP/PTP devices have multiple network ports that could be configured to isolate control traffic. Protections should also be put in place to verify that PNT input signals conform to service interface specifications and prevent internal data corruption. Consider PNT receivers certifiably capable to execute data integrity checks according to the specified valid range in IS-GPS-200, to verify integrity and resilience. 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 (when two or more PNT systems disagree). Consider PNT systems that employ authentication and encryption of PNT data to preserve integrity and resist spoofing. Consider using an ensemble of multiple PNT sources to improve PNT data integrity and to estimate data uncertainties. Consider using PNT receivers that can verify that the data has been produced by a trusted identity and has not been modified. Consider PNT receivers that execute data integrity checks and IS/ICD/Data compliance checks to verify integrity and resist	**IEEE 1139** **IEEE 1193** **IEEE 1588** 16.14, Annex P.2.2 **IEEE 1952** **IEEE 2030.101** 5 **IETF 5906** 4 **IETF 7384** 5.1-5.3, 5.7-5.9 **IETF 8633** 4, 5 **IETF 8915** 1, 3-9 **IETF NTS** 1-10 **IMO 1575** Appendix C **ISO/IEC 17025** **IS-GPS-200** **IS-GPS-705** **IS-GPS-800** 3 **NIST SP 800-53 Rev. 5** AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-8, SC-11, SC- 12, SC-13, SC- 31, SI-4, SI-7, SI-10, SI-14 **NIST SP 800-160 Rev. 1** 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F **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,

Protect Data Security Subcategory	Applicability to PNT	References (PNT-Specific)
	spoofing. Consider isolation of the inputs and the system outputs to preserve PNT data integrity through autonomous and independent references embedded in the device (i.e., holdover or inertial navigation) which are periodically corrected with autonomously managed PNT outputs between corrections.	2.5.9 **USG FRP** 3.2.5, 3.2.6, 4.3, A.1 **DHS-Integrity** **ITU-8272.2**
PR.DS-10 The confidentiality, integrity, and availability of data-in-use are protected**.**	Confidentiality protects the PNT data-in-use from exposure to unauthorized parties. Mitigation strategies include, but are not limited to protection of memory registers, obfuscation, or encryption. PNT data-in-use can be critical for real-time decisions. Integrity of the PNT data-in-use can be verified through signal authentication and continuous cross-validation with complementary PNT data to assess feasibility of solutions. The ability to adapt PNT data flows in real-time can reduce performance degradation. Assurance in the availability of PNT data-in-use can be strengthened through system resilience including verified redundancy and failover, holdover, and interference mitigations. Special attention must be paid to PNT data which is bound to or used in conjunction with potentially sensitive data, such as PII. *Hold for discussion with small group and public comment discussion*	**3GPP-TR23.271** 4 **3GPP-TS36.305** 8.1 **5GAA-T4CAV** 3 **DHS RFI** **DOT-PNT-SP** **NIST TN 2187** **IETF 8915** 1, 8, 9 **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

4.3.4. Platform Security (PR.PS)

The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability. In the context of this PNT

604 Profile, the PNT data and services are subject to the security policies of the information the PNT data is bound or associated with (e.g.,
605 PII, location of critical assets). There are four PR.PS Subcategories that apply to the PNT Profile, as summarized in Table 12.

606 **Table 12. Protect - Platform Security Subcategories Applicable to PNT**

Protect Platform Security Subcategory	Applicability to PNT	References (PNT-Specific)
PR.PS-01: Configuration management practices are established and applied.	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. 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. 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. Verify that the baseline configuration results in a system that meets the baseline PNT performance requirements, such as uncertainty, wander, and jitter tolerances. PNT deployment should employ the principle of least functionality.	**3GPP TR22.878** 4, 5 **Defraigne 2022** 3, 4 **DHS CISA** 4.b, 5.b **DHS GPS CI** 11 **DHS CISA** 4 **DHS GPS CI** **DHS RCF** 8 **GPS-SPS** 2.4 **ICAO 9849** 5, 6.4, Appendix F **IEEE 1139** **IEEE 1193** **IEEE 1588** Annex N, P **IEEE 2030.101** 4.6-4.13, 4.15, 6, Annex G.2.4 **IETF 5906** 5 **IETF 7384** 7.3 **IETF 8633** 2-9, A.3, A.4 **IETF 9327** 6 **IMO 1575** C.1, E

Protect Platform Security Subcategory	Applicability to PNT	References (PNT-Specific)
	Configure the PNT system to provide only essential capabilities. When PNT data or services do not require functionality from intermediary nodes, they can be disabled to minimize attack surfaces. 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. Calibration procedures may include the absolute or relative calibration or recalibration of components. Document procedures for minimum periodic 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). 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. Enforce approval requirements, control, and monitoring of remote maintenance activities. Employ the appropriate level of authentication, least privilege, logging, record keeping, and session termination for remote	**ISO 15288** 6.3.5 **ISO/IEC 17025** **ITU G. 8272** I.1 **ITU-T G.8275** 7, 8 **ITU-T GNSS** 2, 4, 5, Appendix V, VII **Levine** 2021 **NIST SP 800-53 Rev. 5** AC-3, CM-1, CM-2, CM- 3, CM-4, CM5, CM-6, CM-7, CM-9, SA-10, MA-1, MA-2, MA- 3, MA-4, MA-5, MA-6, SI-13 **NIST SP 800-160** 3.4.9, 3.4.10, 3.4.11 Appendix F, G **NIST SP 1065** 5-10 **NTP SEC** **RTCA 229** 2.2.1.1, 2.4.1, 2.5.2, 2.5.3, 2.5.4, 2.5.7, 2.5.11 **RTCA 235** 2.5.2.1, 2.5.2.2, Appendix G **RTCA 356** 3.5, 3.6, 5.6.1, 5.6.4, 5.6.5 **USG FRP** Appendix A

Protect Platform Security Subcategory	Applicability to PNT	References (PNT-Specific)
	maintenance.	
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.	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. Verify PNT system after firmware and software changes. PNT systems can be returned to a proper working state, and should comply with the latest standards. 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.	**DHS CISA** 4.b **IEEE 2030.101** 4.5, 4.6 **ISO 18305** 6-8, Annex B **NIST SP 800-53 Rev. 5** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-15, SA-17, SI-7, SI-12, SI-14, SI-16, SI-17, MA-1, MA-2, MA- 3, MA-5, MA-6 **NIST SP 800-160 Rev. 1** 3.2.1, Appendix F.3 **RTCA 326** 4.2 **USG FRP** 1.4, 1.7.2
PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk.	An operational system development life cycle for PNT services is established to incorporate and manage security measures throughout the life cycle of components. For critical systems, consider verifying and validating PNT systems, components, and procedures through tests, measurements, inspections, and continuous monitoring. Schedule, perform, record, and review records of maintenance and repairs on PNT devices and components. 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. Employ configuration change control for PNT devices and	**DHS GPS CI** **IEEE 1588** Annex N **IMO 1575** C.1, E.3 **NISTIR 8320** **NIST SP 250-29** **NIST SP 800-53 Rev. 5** CM-3, CM-4, PE-11, SA-10, SI-13, SI-17 **NIST SP 800-160 Rev. 1** 3.3.5 **RTCA 356** 3.8.3, 3.8.4

Protect Platform Security Subcategory	Applicability to PNT	References (PNT-Specific)
	components that are consistent with the software development life cycle to maintain a functioning baseline and monitor all changes to validate impacts and integrity. Prior to deploying a change, conduct impact analyses. Identify and record the effects of impact on downstream applications, users, and downtime. Select, use, and ensemble complementary PNT services based on system priority classifications to meet business continuity objectives. 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, rigorously test and evaluate 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. Change control and maintenance procedures should include documentation and artifacts that will impact the performance of the PNT system, such as calibration procedures. Verify PNT device calibration, status, orientation (e.g., antenna positioning), and actual state compared to the desired state. Consider standards-based mechanisms, such as Trusted Platform Modules (TPM) and other device attestation measures when warranted and practical.	
PR.PS-04 Log records are generated and made available for continuous monitoring.	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.	**Defraigne 2022** 5 **DHS CISA** 7.a **DHS GPS CI**

Protect Platform Security Subcategory	Applicability to PNT	References (PNT-Specific)
	Log entries of proper working states, anomalies, and events. Wherever practical, logging and audit mechanisms should produce data elements in accordance with standard data formats to facilitate parsing and consumption by analytic teams. PNT-dependent applications that require an audit trail often require legal or metrological traceability meaning an unbroken documented chain of calibrations from a standard or other trusted reference. 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.	**DOT 12464** **IEEE 1588** 16.14. III, IV, V 4.4.2 **Matsakis** 2018 **NIST SP 800-53 Rev. 5** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU- 16 **NIST SP 800-160 Rev. 1** 3.3.2, 3.3.5 **SEC 613**

4.3.5. Technology Infrastructure Resilience (PR.IR)

Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience. There are four PR.IR Subcategories that apply to the PNT Profile, as summarized in Table 13.

Table 13. Protect - Technology Infrastructure Resilience Applicable to PNT

Protect Technology Infrastructure Resilience Subcategory	Applicability to PNT	References (PNT-Specific)
PR.IR-01 Networks and environments are protected from unauthorized logical access and usage.	Identify and control connections between system components. Monitor and control connections and communications at the external boundary and at key internal boundaries. Information assurance (IA) measures to preserve PNT service integrity can 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. Consider the isolation of control plane, user plane, and signaling plane where appropriate and practical.	**DHS CISA** 1.a, 4.a **IEEE 1588** Annex P **IETF 5906** 6 **IETF 7384** 5.2 **NIST SP 800-53 Rev. 5** AC-4, SC-7, SC-10
PR.IR-02 The organization's technology assets are protected from environmental threats.	Clocks, clock / communication signals, and communication mediums can be susceptible to environmental perturbations. When applicable, test and monitor for changes in temperature, electromagnetic and RF interference, vibrations, etc., which can cause jumps and drifts in the timing signals or degrade multilateration. Solar storms and ionospheric scintillations can degrade or block RF antenna signal reception. Lightning, snow accumulation, can also impact RF signals. Protect, monitor, and maintain environmental conditions where feasible. Protections include oven- or temperature-controlled crystal oscillators, cable and system shielding, climate control, vibration	**ICAO** 5 **IEEE 1139** **IEEE 1193**

Protect Technology Infrastructure Resilience Subcategory	Applicability to PNT	References (PNT-Specific)
	dampening mounts, lightning arrestors, etc. Test PNT services based on the range of temperature and environmental conditions for the range of applicable use cases.	
PR.IR-03 Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	Consider and prioritize requirements in the context of safety, operational criticality, cost, and other resource availability. Mechanisms include proactive measures that reject spurious 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, adaptive spatiotemporal signal processing, features to limit performance degradation, and to expedite recovery. Approaches include antenna and frontend designs, adaptive spatiotemporal processing techniques, sensor fusion with built-in fault monitors, validation of demodulated data from received GPS signals. Consider system architectures that ensemble multiple sources into a coherent network to limit exposure to threat surfaces, protect internal states, and have intelligent control algorithms. Some mechanisms to consider in the design phase include leveraging PNT service providers with hardened signals, diverse PNT sources in accordance with mission resiliency requirements. 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. Resiliency requirements permit an organization to determine if the full capability of its current PNT service provider is needed. For	**3GPP TS 22.261** 6.36, 7.8 **3GPP TS 22.878** 4, 5 **5GAA-PAAS** 6 **DHS CISA** 6 **DHS PNT** III-V **DHS RCF** 5, 6 **DHS SG** **DHS S&T 2022** 3-5 **DOT-CPNT-AP** **DOT-PNT-SP** **GPS GNSS2** **GPS SPS** 3 **IEEE 1588** 9.3, 16.4, 17 **IETF 8633** 3.2, 3.3 **IMO 1575** C.2.1, C.2.2 **ITU-T G.8262** 11 **ITU-T G.8272** 7 **ITU-T G.8272.1** 8, Appendix I-V

Protect Technology Infrastructure Resilience Subcategory	Applicability to PNT	References (PNT-Specific)
	example, if relative time synchronization or frequency synchronization is sufficient, then an organization may have more complementary holdover reference options. PNT applications requiring only a relative frame of reference may have additional resilience capabilities using local sensors, signals of opportunity, computations, and communications. 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.	**ITU-T G.8272.2** 6-10, Annex A, Appendix I **ITU-T G.8275.1** Appendix VII **NIST SP 800-53 Rev. 5** CP-2, CP-7, CP-8, CP-10, CP- 11, CP-12, CP-13, PE-11, RA-9, SA-8, IR-4, IR-8 **NIST TN 2187** **RTCA 229** 2.1.1, 2.1.2, 2.1.4, 2.5 **RTCA 235** 14.2, 14.3, 14.4 **USG FRP** 1.7, 5.1, 6
PR.IR-04 Adequate resource capacity to ensure availability is maintained.	Determine required performance levels of PNT data regardless of environmental threats or if applications can rely on alternatives without the PNT data (systems/components). Determine PNT data traceability requirements and reconcile with the PNT data performance (e.g., accuracy, integrity, continuity, availability, coverage) for the software, applications, systems, and operating environment. 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. All sources of PNT, including alternate or complementary PNT	**3GPP TR22.878** 4, 5 **3GPP TS36.305** 4.3 **DHS RCF** 3, 5.3, 5.4 **DHS PNT** IV, V **GPS GNSS** **GPS USER** **ICAO 9849** 2.2.3, 2.2.4, 5.1, 6.2, Appendix G **IEC 62439-3** 4, 5 **IEEE 1588** Appendix P.2.3 **IEEE 2030.101** 4.6, 4.8, 4.9, 4.12, 4.13 **IETF 7384** 5.4

Protect Technology Infrastructure Resilience Subcategory	Applicability to PNT	References (PNT-Specific)
	devices, need to be tested and enabled in advance of a PNT disruption event. Where needed, incorporate measures such as stand-alone and holdover capabilities or other means for deriving PNT data when PNT sources are unavailable.	**ITU-T G.8262** 11 **ITU-T G.8275** 7.2 **Kaplan** 1.8, 12, 13 **NIST SP 800-53 Rev. 5** AU-4, CP-2, PE-11, SC-5, SC-6 **NIST TN 2187**

4.4. Detect Function

The Detect Function addresses the development and deployment of appropriate activities to find and analyze possible cybersecurity attacks. The Detect Function is informed by the Identify Function and is enabled by the Protect Function under the policies and risk strategy determined by the Govern Function.

The Detect Function defines two Categories, both of which have Subcategories that apply to the PNT Profile to varying degrees, as summarized in Sec. 4.4.1 through Sec. 4.4.2.

4.4.1. Continuous Monitoring (DE.CM)

The information system and assets are monitored to find and analyze possible cybersecurity attacks and compromise. In the context of this PNT Profile, this might include monitoring 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.

There are four DE.CM Subcategories that apply to the PNT Profile, as summarized in Table 14.

622 **Table 14. Detect – Security Continuous Monitoring Subcategories Applicable to PNT**

Detect Security Continuous Monitoring Subcategory	Applicability to PNT	References (PNT-Specific)
DE.CM-01: Networks and network services are monitored to find potentially adverse events.	Monitor the PNT source(s) 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-related security measures may fail. Monitor user activities, the distribution characteristics (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 when the system needs to fail-secure or fail-safe. Heighten system monitoring activities when there is an indication of increased risk. Use an effective mix and fusion of data from multiple, diverse PNT sources and PNT data distribution routes. 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. 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	**DHS CISA** 1.d, 4.a **DHS Integrity** **DHS RCF** 7, 8 **DOT 12464** **GDGPS** **ICAO 9849** 5.3.1.5-5.3.1.9, 7.8 **IEEE 1588** 16.11, 16.12, Annex J, M, P.2.4 **IEEE 2030.101** 4.5.2 **IETF-9327** **IMO 1575** C.2.2, Appendix C.1 **ITU-T GNSS** Appendix III, VI **NIST SP 800-53 Rev. 5** AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, PM-31, SC-5, SC-7, SC-18, SI-4, SC-44, SI-3,SI-4,SI-8 **NTP MON** **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 **RTCA 235** 2.3, 2.5 **USG FRP** Appendix B

Detect Security Continuous Monitoring Subcategory	Applicability to PNT	References (PNT-Specific)
	applications and users. 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. Consider providing a loopback reference timing signal to continuously monitor for changes in the total network and signal propagation delay. High precision clock signals can be applied to detect changes in path delay as a measurement method to detect anomalies in the communication channel. Within a specified time, alert dependent users and applications when monitoring is unavailable or when PNT data or service is unavailable. Software and hardware can be integrated into the PNT system and critical infrastructure components to detect and mitigate GNSS jamming and spoofing events and preserve PNT data availability, continuity, and integrity. Deploy malicious code detection mechanisms, such as behavioral anomaly detection tools, throughout the PNT systems to detect and eradicate malicious code. Should an application dependent on PNT data experience an anomaly, consider investigating the PNT source and associated user applications as possible sources of the anomaly. Systems that use and support PNT data should be included in antivirus analysis. Update malicious code protection mechanisms, such as antivirus protections, when new releases are available in accordance with the	

Detect Security Continuous Monitoring Subcategory	Applicability to PNT	References (PNT-Specific)
	configuration management policy and procedures for the PNT systems involved. 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. Conduct ongoing security status monitoring on PNT systems for unauthorized personnel, connections, devices, access points, and software. Monitor for system inventory discrepancies.	
DE.CM-02: The physical environment is monitored to find potentially adverse 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. 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** **ICAO 9849** 5.3.7 **Kaplan** 10 **NIST SP 800-53 Rev. 5** CA-7, PE-6, PE-20 **DHS-RFI** **IATA-RFI**
DE.CM-03: Personnel activity and technology usage is monitored to find potentially adverse 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

Detect Security Continuous Monitoring Subcategory	Applicability to PNT	References (PNT-Specific)
DE.CM-06: External service provider activities and services are monitored to find potentially adverse 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. 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), and CGSIC (Civil GPS Service Interface Committee) bulletins. Additional sector- specific advisories may be provided by ISACs and sector-specific agencies.	**DOT CMPS** 3 **IS-GPS-200** 3 **IS-GPS-705** 3 **IS-GPS-800** 3 **ICAO 9849** 7.8, 7.11 **IMO 1575** 2.2, B.1, E.1 **NAVCEN** **NIST SP 800-53 Rev. 5** CA-7, PS-7, SA-4, SA-9, SI-4 **USG FRP** Appendix B

4.4.2. Anomalies and Events (DE.AE)

Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. 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 DE.AE Subcategories that apply to the PNT Profile, as summarized in Table 15.

628 **Table 15. Detect – Anomalies and Events Subcategories Applicable to PNT**

Detect Anomalies and Events Subcategory	Applicability to PNT	References (PNT-Specific)
DE.AE-02: Potentially adverse events are analyzed to better understand associated activities.	Review and analyze detected events within the systems using PNT data 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. Be able to distinguish between potentially harmful events and normal operations. Be able to predict harm based on events. Consider systems using PNT data when analyzing cybersecurity events involving downstream applications. For RFI, include environmental monitoring with direction- finding capabilities to locate the source. Preserve the raw data, analysis, and characterization to aid in the analysis of future events.	**DHS GPS CI** **DHS RCF** 5.2 **DOT SP** **Kaplan 2017** Chapters 9, 10 **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, RA-5, SI-4 **RTCA 229** Appendix R **RTCA 235** 2.1 **DHS-RFI** **IATA-RFI**
DE.AE-03: Information is correlated from multiple sources.	Multiple sensors and sources can be used to correlate fault modes and contribute to anomaly models and algorithms. PNT data from multiple sources may be used, cross-checked, and compared for the detection of anomalous behavior. Compile sufficient event data across the systems using PNT data using various sources, such as event reports, logs, audit monitoring, network monitoring, physical access monitoring, environmental monitoring, and user and administrator reports. Standards-based data formatting and serialization promotes the communication interoperability and interchangeability of PNT data and supporting data. Consider subscribing to or enabling user community and PNT	**DHS SP** **GPS ICD-870** 3.1 **GPS USER** **ICAO 9849** 5.3.3.5, 7.11 **IEEE 1588** Annex J **IEEE 2030.101** 4.7, 4.8, 4.13, 5.4.4 **IETF-9327** **IMO 1575** 2, 3 **NAVCEN**

Detect Anomalies and Events Subcategory	Applicability to PNT	References (PNT-Specific)
	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 sector-specific agencies.	**NIST SP 800-53 Rev. 5** AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4 **NIST SP 800-160 Rev. 1** 3.3.7 **RTCA 229** Appendix G.2, G.3 **RTCA 235** 1.1 **SPD-7** **USG FRP** Appendix A
DE.AE-04: The estimated impact and scope of adverse events are understood.	Identify the effects of anomalous events on the PNT data and systems 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** **NIST SP 800-53 Rev. 5** CP-2, IR-4, RA- 3, SI-4 **RTCA 229** Appendix R
DE.AE-06 Information on adverse events is provided to authorized staff and tools.	Keep apprised of potential and scheduled disruptions from PNT service providers. Communicate PNT data anomaly detection and the current best estimate of PNT data quality to personnel, partners, analytics, and downstream application users. 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 **IEEE 1588** 7.6.2, 16.11, 16.12 **IEEE C37.238** 6.2.1, 6.3 **IETF-9327** **IMO 1575** 2.3, B.2.2.1 **ITU-T G.8275** Appendix II, IV **NAVCEN** **NIST SP 800-53 Rev. 5** AU-6, CA-2, CA-7, RA5, SI-4 **RTCA 229** 2.1.1.4

Detect **Anomalies and Events** **Subcategory**	**Applicability to PNT**	**References (PNT-Specific)**
		USG FRP Appendix B **FCC**
DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria.	Establish PNT incident thresholds and understanding of potential impacts to the mission and enable proper reporting, alerting thresholds, and the development of adequate incident alert procedures. 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 time upon nearing and exceeding thresholds. Based on mission requirements, consider reviewing and revising thresholds on a routine basis.	**GPS SPS** 2.3.4 **ICAO 9849** 7.11 **IMO 1575** 2.2.1, Appendix C **NIST SP 800-53 Rev. 5** IR-4, IR-5, IR-8 **USG FRP** Appendix A

4.5. Respond Function

Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication. The activities in the Respond Function support the ability to contain the impacts of a disruption or manipulation to PNT services or data.

The Respond Function creates recommended actions and is triggered by the outputs generated by activities from the Detect Function. The Protect Function provides the ability for the Respond Function to execute the proper response to an event according to a predefined plan.

The Respond Function within the Cybersecurity Framework defines four Categories, all of which have at least one Subcategory that applies to the PNT Profile to varying degrees, as summarized in Sec. 4.5.1 through Sec. 4.5.4.

4.5.1. Incident Management (RS.MA)

Responses to detected cybersecurity incidents are managed.

There are three RS.MA Subcategories that apply to the PNT Profile, as summarized in Table 16.

Table 16. Respond – Incident Management Subcategories Subcategory Applicable to PNT

Respond Incident Management Subcategory	Applicability to PNT	References (PNT-Specific)
RS.MA-01 The incident response plan is executed in coordination with relevant third parties once an incident has been declared.	Execute response plans during or after a cybersecurity event that affects PNT systems in accordance with the predefined threshold. In the event of PNT disruption or manipulation, coordinate PNT cybersecurity incident response actions with all relevant stakeholders in accordance with predefined agreements and the incident response plan. When agreed upon between stakeholders, common data formats facilitate information sharing to strengthen the protection of the user community. This should be documented in the relevant incident response plans.	**NERC EISAC** **NIST SP 800-53 Rev. 5** IR-4 **NIST SP 800-61 Rev. 3** 2.3 **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8, PE-6
RS.MA-02 Incident reports are triaged and validated.	Investigate incident reports generated from PNT anomaly detection systems. Identify and locate potential sources of RFI. 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	**IATA FDX** **IATA IDX** **ICAO 9849** 3, Appendix F 6.2 **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, PE-6, RA-5, SI-4 **RTCA 235** 14.1.2 **DHS-RFI** **FCC**

Respond Incident Management Subcategory	Applicability to PNT	References (PNT-Specific)
	interference. 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. Understand the full implication of an incident report based on thorough investigation and analysis results. Consider the organizational impacts on PNT services that may affect downstream applications, users, and systems that are dependent on PNT. Understand downstream impacts and relationships through leveraging mapped services and outlined policies. Understand the scope and necessary actions required for remediation.	
RS.MA-03 Incidents are categorized and prioritized.	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 **NIST SP 800-61 Rev. 3** 2, 3.2 **DHS-RFI**

4.5.2. Incident Analysis (RS.AN)

Investigations are conducted to support effective response, forensics, and 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 four RS.AN Subcategories that apply to the PNT Profile, as summarized in Table 17.

Table 17. Respond – Incident Analysis Subcategories Applicable to PNT

Respond Incident Analysis Subcategory	Applicability to PNT	References (PNT-Specific)
RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident.	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. Conduct forensic analysis to aid in determination of the root cause of PNT disruption or manipulation. Include various in-situ and historic data in the forensic analysis when a PNT event happens to identify the source. Historic information can be applied to advanced trend detection and included in response audits.	**ICAO 9849** Appendix F 6.2 **NIST SP 800-53 Rev. 5** AU-7, IR-4 **NIST SP 800-61 Rev. 3** 3.2
RS.AN-06 Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved.	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.	**NIST SP 800-53 Rev. 5** CP-2, IR-8
RS.AN-07 Incident data and metadata are collected, and their integrity and provenance are preserved.	Maintain a PNT incident database in order to inform future mitigation strategies. Relevant data and contextual PNT metadata such as, but not limited to, timestamps, signal power levels, signal to noise ratio, receiver position, and signal time and direction of arrival can support incident analysis. Use of authenticated signals verifies the PNT metadata is from a	**5GAA PAAS** 6 **DHS RCF** 5.4 **GSC OSNMA** **IATA FDX** **IATA IDX**

Respond Incident Analysis Subcategory	Applicability to PNT	References (PNT-Specific)
	specific source. Complementary PNT sources, including onboard holdover clocks and multi-modal positioning, such as IMUs, lidar, radar, ultra-wideband positioning, can be used to verify the integrity of the metadata.	**IEEE 1588** Annex P
RS.AN-08 An incident's magnitude is estimated and validated.	Analyze the impact of the PNT data anomaly on user and application errors. 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 and incident response plans. Characterize nominal and anomalous PNT data from the incident for improving future monitoring and detection. Incident data and metadata can be analyze using simulators and test suites to estimate and validate the magnitude of the impact on PNT data and application performance. PNT data affected by an incident could rely on incident data, metadata, and other sources of precise time, location, and cross-referencing to determine the incident's magnitude, and how the PNT incident was caused.	**DHS Integrity** **ICAO 9849** 3 **NIST TN 1366**

4.5.3. Incident Response and Communication (RS.CO)

Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies. In the context of this PNT Profile, external stakeholders may include sources of PNT data as well as sources that announce events that will impact the PNT service, such as PNT interference or corrections for leap seconds.

There are two RS.CO Subcategories, and both apply to the PNT Profile, as summarized in Table 18.

652 **Table 18. Respond - Communications Subcategories Applicable to PNT**

Respond Communications Subcategory	Applicability to PNT	References (PNT-Specific)
RS.CO-02: Internal and external stakeholders are notified of incidents.	Ensure that cybersecurity events on the PNT system are reported in a manner consistent with the response plan. Suspected intentional or unintentional interference should be reported to stakeholders through the appropriate channels and procedures. For example, suspected RFI can be reported to NAVCEN, National Aeronautics and Space Administration (NASA) Aviation Safety Reporting System for aeronautics, or the North American Electric Reliability Corporation (NERC) E-ISAC for the electric utility sector. 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.	**DHS CISA IE** **DHS RFI** **FCC** **GPS USER** **ICAO 9849** 3, 7.12, Appendix F 6.1.1 **NAVCEN** **NIST SP 800-53 Rev. 5** AU-6, IR-6, IR-8 **NIST SP 800-61 Rev. 3** 3.2 **NERC CIP-008-6** **NERC EISAC** **USG FRP**
RS.CO-03: Information is shared with designated internal and external stakeholders.	Share cybersecurity incident information with relevant stakeholders as defined in the organizational sharing policies. 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 **FCC** **GPS USER** **ICAO 9849** 7.11, 7.12, Appendix F 6.1.1 **IEEE 1588** 7.6.2, 16.11, 16.12 **NAVCEN** **NERC EISAC** **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8 **NIST SP 800-61 Rev. 3** 2.3

Respond Communications Subcategory	Applicability to PNT	References (PNT-Specific)
		DHS-RFI

4.5.4. Incident Mitigation (RS.MI)

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 two RS.MI Subcategories that apply to the PNT Profile, as summarized in Table 19.

Table 19. Respond – Incident Mitigation Subcategories Applicable to PNT

Respond Incident Mitigation Subcategory	Applicability to PNT	References (PNT-Specific)
RS.MI-01: Incidents are contained.	Contain cybersecurity incidents to minimize impacts on the PNT system. 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. PNT system response to anomaly may include failover to back-up sources. Validate and verify the most effective failover	**DHS GPS CI** **NIST SP 800-53 Rev. 5** IR-4 **NIST SP 800-61 Rev. 3** 3.4.1

Respond Incident Mitigation Subcategory	Applicability to PNT	References (PNT-Specific)
	mechanisms such as, but not limited to those based on source priorities, voting, or a weighted reference ensemble prior to including it in the response plan.	
RS.MI-02: Incidents are eradicated.	Once the effects of the incident are contained, (1) implement PNT-based mitigation measures that can include alternate or complementary sources in order to operate through the incident; and (2) 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. Apply patches and updates to mitigate the vulnerability or incident. Consider and validate the operational impacts of the modifications. Mitigation procedures or measures should be part of the business continuity plan. Consider mitigation strategies such as PNT source and data path redundancy, diversity, and segmentation to minimize the impacts of PNT disruption or manipulation. 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.	**3GPP TR22.878** 4, 5 **DHS GPS CI** **DHS RCF** 5.3, 5.4 **ICAO 9613** 6.3.7.1 **IMO 1575** C.2.1, C.2.2 **ITU-T G.8262** V **ITU-T G.8272** 7 **Kaplan** 1.8, 13 **NIST SP 800-53 Rev. 5** IR-4 **NIST SP 800-61 Rev. 3** 3.4 **NTP SEC** **USG FRP** 4

4.6. Recover Function

The Recover Function implements the appropriate activities to ensure that assets and operations affected by a cybersecurity incident are restored.

The activities in the Recover Function support timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

The Recover Function within the NIST Cybersecurity Framework has two Categories, only one of which is relevant to the use of PNT data.

4.6.1. Incident Recovery Plan Execution (RC.RP)

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

There are four RC.RP Subcategories that apply to the PNT Profile, as summarized in Table 20.

Table 20. Recover – Incident Recovery Plan Execution Subcategories Applicable to PNT

Recover Incident Recovery Plan Execution Subcategory	Applicability to PNT	References (PNT-Specific)
RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process.	The business continuity plan should include a recovery plan. Execute the recovery plan during or after a cybersecurity incident on the PNT system to adhere to recovery time and recovery point objectives.	**ICAO 9849** 7.4 **NIST SP 800-34 Rev. 1** 2.2.1, 3.2 **NIST SP 800-53 Rev. 5** CP-10, IR-4, IR-8
RC.RP-02 Recovery actions are selected, scoped, prioritized, and performed.	The recovery plan can include specific actions for restoration, recalibration, resetting, and test validation of equipment.	**IEEE 1686** 5.5.3 **IEEE 2030.101** 4.15.2, 4.15.3 **NIST SP 800-34 Rev. 1** 3.5 **RTCA 229** 2.1-2.4

RC.RP-04 Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norm.	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.	**IEEE 1686** 5.6 **NIST SP 800-34 Rev. 1** 2.2.2 **NIST SP 800-160 Rev. 1** Appendices E.24, F.2 **NIST SP 800-184** **RTCA 229** 2.1-2.4
RC.RP-05 The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.	Restore and re-calibrate PNT assets from a known, good offline configuration files in an isolated environment. Perform PNT system acceptance testing, and verify normal operations, signal, and data integrity prior to propagating PNT information downstream to critical applications. Signal and data integrity verification can rely on agreement among multiple PNT sources. Discontinuities in the data can indicate potential compromise. Normal operations can be defined by the accuracy, precision, stability, and signal-to-noise ratios.	**DHS-Integrity** **ICAO 9849** 7.7 **NIST SP 800-184** 3.1 **RTCA 229** 2.5

References

[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/SpecificationDetails.aspx?specificationId=3769

[3GPP-TR23.271] 3rd Generation Partnership Project (2025); Functional Stage 2 Description of Location Services (Release 19.0) October 2025. (Technical Specification Group Services and System Aspects, Sophia Antipolis, France). Specification TR.23.271. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=834

[3GPP-TS22.071] 3rd Generation Partnership Project (2025) Location Services (LCS) Service description Stage 1(Release 17) October 2025. (Technical Specification Group Services and System Aspects, Sophia Antipolis, France). Specification 22.071. Version 19.0.0. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=584

[3GPP-TS22.104] 3rd Generation Partnership Project (2024) Service requirements for cyber-physical control applications in vertical domains (Release 19) June 2024. (Technical Specification Group Services and System Aspects, Sophia Antipolis, France). Specification 22.104. Version 19.2.0. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=584

[3GPP-TS22.261] 3rd Generation Partnership Project (2026) Service requirements for the 5G system (Release 20) March 2026. (Technical Specification Group Services and System Aspects, Sophia Antipolis, France). Specification 22.261. Version 20.6.0. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=584

[3GPP-TS36.305] 3rd Generation Partnership Project (2025) 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,) October 2025. Specification TS36.305. Version 19.0.0. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetail s.aspx?specificationId=2433

[5GAA-PAAS] 5G Automotive Association (2026) *Enhanced Positioning Accuracy and Coherent Situational Awareness by Connected Sensors and Positioning as a Service*. (5GAA, Munich, Germany) Available at https://5gaa.org/content/uploads/2026/01/5gaa-consens-technical-report.pdf

[5GAA-T4CAV] 5G Automotive Association (2025) *A Framework for Dynamic Trustworthiness Assessment in Cooperative and Automated Vehicles*. (5GAA, Munich, Germany) Available at https://5gaa.org/content/uploads/2025/08/5gaa-wi-trust4cav-white-paper-10072025-v3.pdf

[ACA 2007] America Competes Act (2007) Public Law 110-69, 15 USC 205. https://www.nist.gov/system/files/documents/2017/05/09/15-USC-205-sec-3570-America-Competes-Act-SI-Excerpt.pdf

[ASPN] Department of Defense (2023) All-Source PNT Network. Available at https://www.aspn.us

[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

[Barret2018] 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*.

[BIPM] Bureau of Weights and Measures (2022) *Realizing and disseminating international reference time scales UTC, UTCr and TT(BIPM)* (BIPM, Paris, France). Available at https://www.bipm.org/en/time-metrology

[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

[Defraigne 2022] Defraigne P, Achkar J, Coleman MJ, Gertsvolf M, Ichikawa R, Levine J, Uhrich P, Whibberley P, Wouters M, Bauch A. Achieving traceability to UTC through GNSS measurements. Metrologia. 2022 Oct 28;59(6):064001. Available at https://iopscience.iop.org/article/10.1088/1681-7575/ac98cb/pdf

[DHS-ACQ] Cybersecurity & Infrastructure Security Agency (2024) Federal Positioning, Navigation, and Timing (PNT) Services Acquisitions Guidance Version 1.0, (DHS, Washington, DC). Available at https://www.cisa.gov/resources-tools/resources/federal-positioning-navigation-and-timing-services-acquisitions-guidance

[DHS-CISA] Cybersecurity & Infrastructure Security Agency (2022) 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_0.pdf

[DHS-CISA-IE] Cybersecurity & Infrastructure Security Agency (2022) Global Positioning System Interference Event, (DHS, Washington, DC). Available at https://www.cisa.gov/sites/default/files/publications/CISA-Insights_GPS-Interference_508.pdf

[DHS-Integrity] Cybersecurity & Infrastructure Security Agency (2021) Positioning, Navigation, and Timing (PNT) Integrity Library, Release 1.1 (DHS, Washington, DC). Available at https://github.com/cisagov/PNT-Integrity

[DHS-SG] Department of Homeland Security. Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience (2024). (DHS, Washington, DC). Available at https://www.dhs.gov/publication/strategic-guidance-and-national-priorities-us-critical-infrastructure-security-and

[DHS-GPS-CI] Department of Homeland Security. Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure (2017). (DHS, Washington, DC). Available at https://www.cisa.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.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-RFI] Department of Homeland Security (2020) Radio Frequency Interference Best Practices Guidebook (DHS, Washington, DC). Available at https://www.cisa.gov/sites/default/files/publications/SAFECOM-NCSWIC_RF_Interference_Best_Practices_Guidebook_6-4-20-FINAL_508c.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-2021] Department of Homeland Security (2021) *GPS Receiver Allow List Development Guide.* (DHS, Washington, DC). Available at https://www.dhs.gov/sites/default/files/2022-11/22_1109_st_gps_allow_list_development_duide_v1.1.pdf

[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-S&T-2025] Department of Homeland Security (2025) *Best Practices for Resilient PNT Supporting Critical Infrastructure Version 1.0.* (DHS, Washington, DC). Available https://www.dhs.gov/science-and-technology/publication/pnt-best-practices-supporting-critical-infrastructure

[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 (2025). *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/civil-gps-service-interface-committee

[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/sites/default/files/2025-07/2020-civil-monitoring-performance-specification.pdf

[DOT-CPNT-AP] Department of Transportation (2024) *Complementary Positioning, Navigation and Timing Action Plan*. (Department of Transportation, Washington, DC). Available at https://www.transportation.gov/pnt/complementary-pnt-action-plan

[DOT-PNT-SP] Department of Transportation (2024) *Positioning, Navigation and Timing Strategic Plan*. (Department of Transportation, Washington, DC). Available at https://www.transportation.gov/pnt/dot-positioning-navigation-timing-pnt-strategic-plan

[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

[FAA-AIM] Federal Aviation Administration (2025) Aeronautical information manual. (Department of Transportation, Washington, DC), August 7,2025. Available at https://www.faa.gov/air_traffic/publications/atpubs/aim_html/index.html

[FAA 1770.68] Federal Aviation Administration (2020) Order 1770.68 - Selection and Use of Time and Frequency Sources for all Systems, Services, and Applications Supporting National Airspace System Operations (Department of Transportation, Washington, DC), November 3, 2020. Available at https://www.faa.gov/documentLibrary/media/Order/FAA_Order_1770.68.pdf

[FAR 52.204] Federal Acquisition Regulation (2025) Part 52 - Solicitation Provisions and Contract Clauses. (General Services Administration, Washington, DC), October 1, 2025. Available at https://www.acquisition.gov/far/part-52#FAR_52_204_24

[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 (2023) *4590. Synchronization of Member Business Clocks.* (FINRA, Washington, DC). Available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/4590

[FINRA-6800] Financial Industry Regulatory Authority (2025) *6800. Consolidated Audit Trail Compliance Rule.* (FINRA, Washington, DC). Available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/6800

[GAL-ICD] European GNSS (Galileo) Open Service (2023) *Signal-in-Space Interface Control Document Issue 2.1.* (European Union). Available at https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.1.pdf

[GDGPS] National Aeronautics and Space Administration (2020) *The Global Differential GPS System* (Jet Propulsion Laboratory, NASA, Pasadena, CA). Available at https://gdgps.jpl.nasa.gov/.

[GPS] Department of Homeland Security, U.S. Coast Guard (1996) *Navstar GPS User Equipment Introduction.* (U.S. Coast Guard Navigation Center, Department of Homeland Security, Alexandria, VA), September 1996. Available at https://www.navcen.uscg.gov/sites/default/files/pubs/gps/gpsuser/gpsuser.pdf

[GPS-GNSS] National Coordination Office for Space-Based Positioning, Navigation, and Timing (2025) *Other Global Navigation Satellite Systems (GNSS).* Available at https://www.gps.gov/other-global-navigation-satellite-systems-gnss

[GPS-GNSS2] National Coordination Office for Space-Based Positioning, Navigation, and Timing (2025) *Use of foreign satellite navigation signals.* Available at https://www.gps.gov/use-foreign-satellite-navigation-signals

[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/sites/default/files/2025-07/2020-SPS-performance-standard.pdf

[GPS-USER] Department of Transportation (2025) *Global Positioning System (GPS) Service Outages and Status Reports*. (Department of Transportation, Washington, DC). Available at https://www.gps.gov/gps-service-outage-status-reports

[GSC-OSNMA] European Union Agency for the Space Programme (2024) *Galileo Open Service Navigation Message Authentication Receiver Guidelines*. Available at https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_Receiver_Guidelines_v1.3.pdf

[IANA-TZDB] Internet Assigned Numbers Authority (2022) *Time Zone Database*. (IANA, Los Angeles, CA). Available at https://www.iana.org/time-zones

[IATA-FDX] International Air Transport Association (IATA) (2026) Flight Data eXchange. (Montréal, Québec). Available at https://www.iata.org/en/services/data/safety/gadm/fdx/

[IATA-IDX] International Air Transport Association (IATA) (2026) Incident Data eXchange. (Montréal, Québec). Available at https://www.iata.org/en/services/data/safety/gadm/idx/

[IATA-RFI] International Air Transport Association (IATA) (2025) GNSS Radio Frequency Interference: Safety Risk Assessment, Version 5. (Montréal, Québec). Available at https://ic.iata.org/sites/default/files/iata_sih_document_attachment/IATA%20Safety%20Risk%20Assessment%20-%20GNSS%20Interference%20V5.pdf

[ICAO-9613] International Civil Aviation Organization (2023) *Doc 9613 Performance Based Navigation Manual.* Fifth edition. (Montréal, Québec). Available at https://store.icao.int/en/performance-based-navigation-pbn-manual-doc-9613

[ICAO-9849] International Civil Aviation Organization (2025) *Doc 9849 Global Navigation Satellite System Manual.* Fifth edition. (Montréal, Québec). Available at https://store.icao.int/en/global-navigation-satellite-system-gnss-manual-doc-9849

[ICD-GPS-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 at https://www.gps.gov/technical/icwg/ICD-GPS-240D.pdf

[ICD-GPS-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

[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-525] IEEE Standards Association (2025) *IEEE Guide for the Design and Installation of Cable Systems in Substations* (IEEE SA, Piscataway, NJ). Available at https://standards.ieee.org/ieee/525/7274/

[IEEE-802.1AS] IEEE Standards Association (2025) *IEEE 802.1AS Timing and Synchronization for Time Sensitive Applications* (IEEE SA, Piscataway, NJ). Available at https://standards.ieee.org/ieee/802.1AS/11968/

[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 (2022) *IEEE 1139:2022 Standard Definitions of Physical Quantities for Fundamental Frequency and Time Metrology---Random Instabilities* (IEEE SA, Piscataway, NJ). Available at https://doi.org/10.1109/IEEESTD.2022.9973001

[IEEE-1193] IEEE Standards Association (2022) *IEEE 1193:2022 IEEE Guide for Measurement of Environmental Sensitivities of Standard Frequency Generators* (IEEE SA, Piscataway, NJ). Available at: https://doi.org/10.1109/IEEESTD.2023.10115258

[IEEE-1686] IEEE Standards Association (2022) *IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities.* Available at https://doi.org/10.1109/IEEESTD.2023.10034445

[IEEE 1952] IEEE Standards Association (2025) *P1952 Working Group: Standard for Resilient Positioning, Navigation, and Timing (PNT) User Equipment.* Available at https://standards.ieee.org/ieee/1952/10606/

[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

[IERS] International Earth Rotation and Reference Systems Service (2022) *IERS Bulletins* (IERS, Paris, France). Available at https://datacenter.iers.org/bulletins.php

[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) 8915. Available at https://tools.ietf.org/html/rfc8915

[IETF-9327] Haberman B (2022) Control Messages Protocol for Use with Network Time Protocol. Internet Engineering Task Force (IETF) Network Working Group), V4. Available at https://tools.ietf.org/html/rfc9327

[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

[IGS-RINEX] International GNSS Service (2025) The Receiver Independent Exchange Format (RINEX), version 4.02. Available at https://igs.org/formats-and-standards/

[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

[IS-AGT-100] Air Force Research Laboratory Space Vehicles Directorate (2024) Interface Specification IS-AGT-100 Rev A Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface. Available at https://www.gpsexpert.net/chimera-specification

[IS-GPS-200] SAIC (GPS SE&I) (2022) *Navstar GPS Space Segment/Navigation User Segment Interfaces*. (Air Force Space Command, Washington, DC), Global Positioning System Interface Specification Document IS-GPS- 200N. Available at https://www.gps.gov/technical/icwg/IS-GPS-200N.pdf

[IS-GPS-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

[IS-GPS-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

[ISO-15288] International Organization for Standardization (2015) *ISO/IEC/IEEE 15288 Systems and software engineering – Life cycle processes* (ISO, Geneva, Switzerland), May. 2015. Available at https://www.iso.org/standard/63711.html

[ISO-15939] International Organization for Standardization (2017) *ISO/IEC/IEEE 15939 Systems and Software Engineering-Measurement Process*. (ISO, Geneva, Switzerland), Apr. 2017. Available at https://ieeexplore.ieee.org/document/7907158

[ISO-16085] International Organization for Standardization (2021) *ISO/IEC/IEEE 16085 Systems and software engineering – Life cycle processes – Risk management*. (ISO, Geneva, Switzerland), Jan. 2021. Available at https://www.iso.org/standard/74371.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

[ISO-17666] International Organization for Standardization (2016) *ISO/IEC 17666 Space systems – Risk management*. (ISO, Geneva, Switzerland), Nov. 2016. Available at https://www.iso.org/standard/69239.html

[ISO-18305] International Organization for Standardization (2016) *ISO/IEC 18305 Real time locating systems-Test and evaluation of localization and tracking systems.*. (ISO, Geneva, Switzerland), Nov. 2016. Available at https://www.iso.org/standard/62090.html

[ISO-27001] International Organization for Standardization (2022) *ISO/IEC 27001 Information security, cybersecurity and privacy protection – Information security management systems - Requirements*. (ISO, Geneva, Switzerland), Oct. 2022. Available at https://www.iso.org/standard/82875.html

[ITRF] International Earth Rotation and Reference Systems Service (2022) *ITRF2020 International Terrestrial Reference Frame*. (IERS International Terrestrial Reference System Centre, Paris, France), Oct. 2022. Available at https://itrf.ign.fr/en/homepage

[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/en

[ITU-T-G.8262] International Telecommunications Union Telecommunications Standardization Sector (2024) *ITU-T G.8262/Y.1367 Timing Characteristics of Synchronous Equipment Clocks.* (ITU-T, Geneva, Switzerland). Available at https://www.itu.int/rec/T-REC-G.8262

[ITU-T-G.8271] International Telecommunications Union Telecommunications Standardization Sector (2020) *ITU-T G.8271/Y.1366 Time and Phase Synchronization Aspects of Telecommunications Networks.* (ITU-T, Geneva, Switzerland). Available at https://www.itu.int/rec/T-REC-G.8271-202003-I/en

[ITU-T-G.8272] International Telecommunications Union Telecommunications Standardization Sector (2025) *ITU-T G.8272/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.8272.1] International Telecommunications Union Telecommunications Standardization Sector (2024) *ITU-T G.8272.1 Timing Characteristics of Enhanced Primary Reference Time Clocks.* (ITU-T, Geneva, Switzerland). Available at https://www.itu.int/rec/T-REC-G.8272/en

[ITU-T-G.8272.2] International Telecommunications Union Telecommunications Standardization Sector (2024) *ITU-T G.8272.2 Timing Characteristics of Coherent Network 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

[Kaplan2017] Kaplan E, Hegarty C. (2017). *Understanding GPS/GNSS: principles and applications.* (Artech House, Boston MA). 3rd ed.

[Levine2021] 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

[Matsakis2018] 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. U.S. Coast Guard (2020) *GPS Problem Reporting.* (DHS, USCG, Washington DC). Available at https://www.navcen.uscg.gov/report-a-problem

[NCAS] Cybersecurity & Infrastructure Security Agency (2026) *National Cyber Awareness Systems.* (DHS, CISA, Washington DC). Available at https://www.cisa.gov/resources-tools/services/national-cyber-awareness-system

[NDAA 889] 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/Section-889-Policies

[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 (2024) The NIST Cybersecurity Framework, Version 2.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.29

[NIST-CSF-OP] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework, Version 2.0 Quick Start Guide for Creating and Using Organizational Profiles. (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://doi.org/10.6028/NIST.SP.1301

[NIST-CSRC] NIST Information Technology Laboratory (2022) Computer Security Resource Center *Glossary*. Available at https://csrc.nist.gov/glossary

[NIST-FIPS-200] 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

[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-ITS] National Institute of Standards and Technology (2026) NIST Internet Time Servers. https://tf.nist.gov/tf-cgi/servers.cgi

[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 NTP] Time Realization and Distribution Group (2026) NIST Authentication NTP Service. https://www.nist.gov/pml/time-and-frequency-division/time-services/nist-authenticated-ntp-service

[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. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=105424

[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 Institute 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] Nelson A, Rekhi S, Souppaya M, Scarfone KA (2025) Incident Response Recommendations and Considerations for Cybersecurity Risk Management (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 3. https://doi.org/10.6028/NIST.SP.800-61r3

[NIST-SP-800-98] Karygiannis T, Eydt B, Barber G, Bunn L, Phillips T (2007) Guidelines for Securing Radio Frequency Identification (RFID) Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-98. https://doi.org/10.6028/NIST.SP.800-98

[NIST SP 800-115] 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 (2022) 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.800-160v1r1

[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 (2024) 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://doi.org/10.6028/NIST.SP.800-161r1-upd1

[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, 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-TN-2189] Lombardi, MA (2021) An Evaluation of Dependencies of Critical Infrastructure Timing Systems on the Global Positioning System. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Technical Note (TN) 2187. Available at https://doi.org/10.6028/NIST.TN.2189

[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

[NMEA-0183] National Marine Electronics Association (2023) Serial data networking, NMEA 0183 version 4.30. Available at https://www.nmea.org/nmea-0183.html

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

[NSM-22] National Security Memorandum (NSM)-22 (2024) National Security Memorandum on Critical Infrastructure Security and Resilience. (The White House, Washington, DC), DCPD-202400358, April 30, 2024. https://www.govinfo.gov/app/details/DCPD-202400358

[NTP-MON] Network Time Protocol (2020) *Who is using my NTP server?* Available at https://support.ntp.org/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/productdetails?id=a1B1R0000092uanUAA

[RTCA-235] Radio Technical Commission for Aeronautics (2022) *RTCA DO-235C 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-236] Radio Technical Commission for Aeronautics (2024) *RTCA DO-236E Minimum Aviation System Performance Standards: Required Navigation Performance for Area Navigation*. (RTCA, Washington, DC). Available at https://my.rtca.org/productdetails?id=a1BPP00000D1h8I2AR

[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 (2024) *RTCA DO-326B - 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

[SAE J2945] SAE International (2020) *SAE J2945/1 Surface Vehicle Standard: On-Board Systems Requirements for V2V Safety Communications*. Available at https://www.sae.org/standards/j29451_202004-board-system-requirements-v2v-safety-communications

[SAE J3161] SAE International (2024) *SAE J3161/1 Surface Vehicle Standard: On-Board Systems Requirements for LTE/V2X Safety Communications*. Available at https://www.sae.org/standards/j29451_202004-board-system-requirements-v2v-safety-communications

[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 (2002) (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

[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.navcen.uscg.gov/nav-pubs-and-documents-general-library

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

[VIM] Joint Committee on Guides in Metrology (2012) International Vocabulary of Metrology – Basic and General Concepts and Associated Terms (VIM 3rd Edition), (BIPM, Cedex France). 200:2012. Available at https://www.bipm.org/en/publications/guides/#vim

Appendix A. Selected Bibliography

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 (2021) *Wide Area Augmentation System.* Available at https://www.faa.gov/sites/faa.gov/files/about/office_org/headquarters_offices/ato/WAAS_QFSheet.pdf

Federal Aviation Administration, U.S. Department of Transportation (2021) *SBAS Worldwide.* Available at https://www.faa.gov/sites/faa.gov/files/2021-12/SBAS_Worldwide_quick_facts.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

Lightman S, Suloway T, Brule J (2022) Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8401 (Draft). Available at https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.ipd.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

McCarthy J, Mamula D, Brule J, Meldorf K (2022) Cybersecurity Profile for Hybrid Satellite Networks (HSN) Cybersecurity. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) 27 (Initial Public Draft). Available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.27.ipd.pdf

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 (2022) *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-026.5-2022_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

Ray J, Senior, K (2005) Geodetic techniques for time and frequency comparisons using GPS phase and code measurements. *Metrologia*, 42(4), 215.

Scholl M, Suloway T (2022) Introduction to Cybersecurity for Commercial Satellite Operations (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8270 (2nd Draft). Available at https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8270-draft2.pdf

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 B. List of Symbols, Abbreviations, and Acronyms

CISA
Cybersecurity and Infrastructure Security Agency

CRPA
Controlled Reception Pattern 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

GDGPS
Global Differential GPS System

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

IERS
International Earth Rotation and Reference Systems Service

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

IT
Information Technology

ITRS
International Terrestrial Reference System

ITRF
International Terrestrial Reference Frame

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

NERC
North American Electric Reliability Corporation

NGS
National Geodetic Survey

NIST
National Institute of Standards and Technology

NOTAM
Notices to Air Missions

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

RPO
Recovery Point Objective

RTO
Recovery Time Objective

SCADA
Supervisory Control and Data Acquisition

SLA
Service-Level Agreement

SP
Special Publication

SPS
Standard Positioning Service

TAI
International Atomic Time

TBS
Terrestrial Beacon System

TESLA
Timed Efficient Stream Loss-tolerant Authentication

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 C. Glossary

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, International Atomic Time (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-800-160-2]

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^{th} of M frequency offset averages over the observation period, τ. 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_0, 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
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 Δt 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 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]

Global Positioning System
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 that 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
An attack that attempts to interfere with the reception of broadcast communications. [CNSSI-4009]

A deliberate communications disruption meant to degrade the operational performance of the RF subsystem. Jamming is achieved by interjecting electromagnetic waves on the same frequency that the reader to tag uses for communication. [NIST-SP-800-98]

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, WGS 84, or the International Terrestrial Reference Frame ITRF2020 [ITRF]. [DOT, adapted]

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]

spoofing
Faking the sending address of a transmission to gain illegal entry into a secure system. [CNSSI-4009]

The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. [CNSSI-4009]

Two classes of spoofing include (1) *measurement spoofing*: introduces signal or signal delay that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change; and (2) *data spoofing*: introduces incorrect digital data to the target receiver for its use in processing of signals and the calculation of PNT. [DHS-GPS-CI, adapted]

Within the context of this document, spoofing includes manipulation of legitimate GNSS signals with intent to corrupt PNT data or signal measurement integrity. For example, it includes, but is not limited to: the transmission of delayed or false GNSS signals with intent to manipulate an asset's computed position or time and frequency.

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

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 D. Applying the PNT Profile to Cybersecurity Risk Management

The PNT Profile can be used to augment an organization's pre-existing risk management program. This section further tailors the PNT Profile in context of a few notional fault scenarios to illustrate how the guidance can be applied to assess and manage PNT related risks in the context of a loss or degradation of PNT data or services. Organizations using the PNT data have the responsibility for mitigating temporary PNT disruptions. An effective PNT risk management strategy provides a dynamic and flexible approach to control risks in evolving environments. Organizations are encouraged to apply the PNT Profile with their risk management approach from concept to acquisitions to acceptance, integration, and deployment, to operations and maintenance. Leveraging the organization's existing risk management program enables a system-level shared context. Furthermore, setting priorities for privacy and security risk management affords additional assurance from component to system implementation.

Each organization selects PNT Profile Subcategories, based on 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 PNT system lifecycle can include the consideration of the acquisition, integration, deployment, operations and maintenance, repair, and replacement of PNT components and services. 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.

Organizations evolve the operational reliability and effectiveness throughout a PNT system's lifecycle by continuously monitoring risks and assessing risk mitigation strategies, such as:

- new techniques and technologies to improve the ability to identify, protect, detect, respond, and recover from PNT system attacks
- the emergence of exploitable PNT vulnerabilities
- methods to mitigate vulnerabilities and operational impacts
- operational environment changes in which the PNT-dependent system is deployed to determine if updates are required to the system's cybersecurity controls

Table 26 illustrates how the PNT Profile can be used by a notional organization to address example scenarios and apply the six Functions of the CSF to manage the risk to PNT systems. Equipment manufacturers and end users can address the scenarios through resiliency and redundancy.

2075

Table 21. Applying the PNT Profile to User Risk Management

Example Scenarios	Govern	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.	*Roles, responsibilities and authorities related to cybersecurity management are established, communicated, understood and enforced.* Activities that users are or are not allowed are documented and communicated to relevant personnel. [GV.RR-02]	*Vulnerabilities, threats, and cyber threat intelligences are identified* related to personnel integrating, maintaining, and relying on PNT user equipment and services. [ID.RA-01, ID.RA-02, ID.RA-03] *Manage PNT user hardware, software, and interface configurations* to include use of configuration management tools, physical inspections, and periodic snapshots. [ID.AM-01, ID.AM-03, ID.AM-07] *Identify improvements in the response, and recovery of PNT data and services* through periodic training and testing of PNT user systems. Incorporate lessons learned, improve technology, and address changes to the organization, PNT system, operating environment, and problems encountered during recovery plan implementation, execution,	*Manage access control to authorized users limited to their roles and responsibilities.* [PR.AA-01, PR.AA-05, PR.AA-06] *Periodically verify administration teams and users have training and experience* in using, testing, and maintaining all available sources of PNT data and signals during normal operations, and properly executing response and recovery plans. [PR.AT-02] *Configuration backups, change control processes,* and *logs of proper working states, anomalies, and events* are established and maintained. *End-to-end systems testing* to verify user configuration after firmware, software, equipment integration and upgrades. [PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04] *Protect networks from unauthorized access and threats.* [PR.IR-01, PR.IR-	Newly deployed or updated PNT data streams are continuously monitored against established PNT data sources to correlate faults. [DE.AE-03] PNT data alert thresholds are established. [DE.CM-06] *Integrity monitoring*. Continuously monitor user actions and related risk management controls. [DE.CM-01]	*Execute response plan.* Apply proper working configuration. Document steps and results. Address changes relative to user interactions with the PNT system, in addition to any configuration changes, in the response plan. Record new threats and vulnerabilities. [RS.MA-01, RS.MI-01, RS.MI-02] *Collect and analyze* incident data and metadata from all PNT sources. [RS.AN-03, RS.AN-06, RS.AN-07] *Alert stakeholders* including downstream users describing the limitations and extent of disruption in PNT source integrity and availability. *Operational constraints* due to PNT data and signal disruptions are *understood and communicated* before	*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. [RC.RP-01, RC.RP-04, RC.RP-05]

Example Scenarios	Govern	Identify	Protect	Detect	Respond	Recover
		and testing. [ID.IM-02, ID.IM-03, ID.IM-04]	02]		continuing operations. [RS.CO-02, RS.CO-03]	
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 and malicious breaches.	*Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.* [GV.RM-03] *Validation and verification of firmware and software upgrades* for PNT services and data. [GV.SC-06] *Assess risks posed by third party software for PNT services and data.* [GV.RM-05, GV.SC-07] NOTE: we could possibly add something under GV.SC-07 on the thought that software is from vendors.	*Maintain inventory of software applications and data flows 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. [ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-06, ID.AM-07] *Identify vulnerabilities and threats* to PNT user software and downstream applications. [ID.RA-01, ID.RA-02, ID.RA-03] *Continuously improve plans* 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,	A *baseline software configuration* adhering to cybersecurity principles for applications providing and using PNT data is applied. *End-to-end systems testing* can verify firmware, software, equipment updates conform to standards and to understand impact of changes on user applications. [PR.PS-01] *Systematic calibration and characterization* procedures of PNT system uncertainty and integrity alert thresholds. [PR.PS-02] Adopt appropriate software assurance methods. Consider verification of PNT systems such as device conformance and systems interoperability testing and certification needed to meet organizational requirements. [PR.DS-01, PR.DS-02, PR.DS-05]	*Event logging* including both normal and anomalous software operating states. [DE.AE-03] *Integrity monitoring*. Continuous monitoring of the PNT device outputs and applications relying on the PNT data from the device and associated risk management controls. [DE.CM-01] PNT data *alert thresholds* are established. [DE.CM-06]	*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. [RS.MA-01, RS.MA-02, RS.MI-02, RS.MI-03] *Collect and analyze* incident data and metadata from all PNT sources. [RS.AN-03, RS.AN-06, RS.AN-07] *Alert stakeholders* including the device manufacturer about software faults or failures describing the limitations and extent of operations disruption and constraints of 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. [RC.RP-01]

Example Scenarios	Govern	Identify	Protect	Detect	Respond	Recover
		and testing. [ID.IM-02, ID.IM-03, ID.IM-04]			services and data. [RS.CO-02, RS.CO-03]	
Hardware: Fault or failure in the PNT user equipment design, or implementation or integration, such as gateware.	*Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.* [GV.RM-03] *Validation and verification of hardware and gateware upgrades* for PNT services and data. [GV.SC-06] *Assess risks posed by third party hardware for PNT services and data.* [GV.RM-05, GV.SC-07] NOTE: we could possibly add something under GV.SC-07 on the thought that software is from vendors	*Inventory all physical devices.* PNT user equipment and intended use, users, applicable regulations, and environment, including baseline performance characteristics, are understood and verified. [ID.AM-01] *Identify vulnerabilities and threats* to assess risks of PNT hardware devices and components. [ID.RA-01 through ID.RA-10] *Update risk assessment.* Improve PNT training, testing, monitoring, detection, response, recovery procedures, and resiliency features. [ID.IM-02]	*Consider redundant or complementary PNT sources.* Consider objective metrics in the recovery plan such as (1) recovery point objective (RPO), which is the maximum tolerable PNT data error and can be applied in determining holdover capabilities of the PNT system; and (2) recovery time objective (RTO), which is how quickly an application must recover following a PNT service disruption. [PR.IR-02, PR.IR-03, PR.IR-04] *Calibration and characterization of PNT system uncertainty* including establishment of testing under operational environmental conditions. [PR.PS-01, PR.PS-03]	*Event logging* including both normal and anomalous software operating states. [DE.AE-03] *Integrity and availability monitoring*. Continuous monitoring of the PNT device outputs and applications relying on the PNT data from the device and associated risk management controls. [DE.CM-01, DE.CM-06] PNT data *alert thresholds* are established. [DE.CM-06]	*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. [RS.MA-01, RS.MA-02, RS.MI-02, RS.MI-03] *Collect and analyze* incident data and metadata from all PNT sources. [RS.AN-03, RS.AN-06, RS.AN-07] *Alert stakeholders* including the device manufacturer about software faults or failures describing the limitations and extent of operations disruption and constraints of 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. *Verify backup PNT sources* are serviceable, operational, and sufficient before continuing operations safely. [RC.RP-01]

Example Scenarios	Govern	Identify	Protect	Detect	Respond	Recover
			Secure physical and remote access to devices. [PR.AC-01, PR.AC-04]		services and data. [RS.CO-02, RS.CO-03]	
Data in transit: Includes adversarial and non-adversarial 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.	*Consider the governance and risk implications of using different sources of PNT data and signals in transit.* Understand and communicate the critical objectives and outcomes PNT users are dependent upon. [GV.OC-03, GV.OC-04, GV.OC-05] *Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.* [GV.RM-03] *Understand and communicate roles and responsibilities for managing cybersecurity risks to users dependent on PNT data or signals.* [GV.RM-03, GV.RR-02] *NOTE not sure there is anything under Govern here*	*Identify PNT signal and data communication threats.* Follow information sources from ISACs and bulletins such as NANUs, Notice to Air Missions (NOTAMs), Safety Information Bulletins (SIBs) to be aware of possible disruption of PNT sources in each area and time frame. Record new threats and vulnerabilities. [ID.RA-01, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, ID.RA-08] *Identify communication resilience capabilities.* Consider how other sensor communications can be leveraged to monitor and detect anomalies in PNT sources. [ID.AM-01, ID.AM-03] *Update risk assessment and recovery plans.* Improve PNT training, testing, monitoring, detection, response,	*Consider multiple communication paths and complementary PNT sources.* A resilient communications network topology can limit the impact of communication attacks. Consider objective metrics in the recovery plan such as RPO and RTO. Additional PNT sources such as NTP and WWVB, and sensors such as INS and IMUs can be used to continue to provide PNT information to the user. [PR.IP-09] *Apply and validate communication technologies* that preserve integrity and improves the reliability and resilience of the PNT information. Consider using controlled reception pattern antenna (CRPA) to reduce impacts of RF interference. Note that such antenna may be subject to export controls. [PR.DS-02, PR.PT-04,	*Integrity monitoring.* Continuous monitoring of the PNT data in transit and control effectiveness. [DE.CM-01] *Event logging* including both normal and anomalous communication states. [DE.AE-03] PNT data *alert thresholds* are established. [DE.AE-04, DE.AE-06]	Execute *contingency procedures* and assess functionality of systems relying on alternative modes of PNT communications. Notify potential PNT data users of availability and integrity impacts. [RS.MA-01, RS.MA-02, RS.MI-02, RS.MI-03] *Collect and analyze* incident data and metadata from all PNT sources. [RS.AN-03, RS.AN-06, RS.AN-07] *Operational constraints* due to PNT data loss are *understood and communicated* before continuing operations. [RS.AN-08] *Alert user community* of PNT signal and data disruptions describing the limitations and extent of disruption to PNT data *integrity and*	*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 services before continuing operations safely. [RC.RP-01]

Example Scenarios	Govern	Identify	Protect	Detect	Respond	Recover
		recovery procedures, and resiliency features. [ID.IM-01, ID.IM-03, ID.IM-04]	PR.IR-04] *Calibrate and characterize PNT system uncertainty*. [PR.PS-02, PR.PS-03]		*availability.* [RS.CO-02, RS.CO-03]	
Supply chain: 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 modified.	*Assess PNT user equipment context of the time and position data integrity and availability.* Review technology control tools and lists to verify suppliers. Conduct empirical verification. Assure total uncertainty meets mission critical requirements. *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. [GV.SC-03, GV.SC-04, GV.OC-04] *Clarify monitoring and detection responsibilities* among to analyze and support root cause determination of anomalous PNT data or signal output. [GV.RR-02]	*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. [ID.AM-05, ID.IM-04] *Suppliers and third-party testing and certification*. Consider relevant conformance testing, certification requirements, and processes. [ID.RA-01, ID.IM-02, ID.IM-04] Assure *the total uncertainty* remains within industry standards and regulatory requirements. [ID.RA-04]	*Suppliers and third-party partners understand their roles and responsibilities.* Provide periodic training for specialized roles in deploying and maintaining PNT user systems and services. [PR.AT-02] *Hardware component authentication* such as radio-frequency identification (RFIDs), physically unclonable functions (PUFs), or other markers. [PR.AA-03] *Hardware lifecycle management* can include, but not limited to, consideration of the acquisition, integration, deployment, operations and maintenance, repair, and replacement of PNT components and services. [PR.PS-03]	*Understand risk impacts among supply chain partners*. Policies and procedures, including lessons learned over time, are adequately documented and shared with stakeholders. [DE.AE-04] PNT data *alert thresholds* are established. [DE.AE-08] *Verify PNT device integrity*. Identify and document known limitations. [DE.AE-02]	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. [RS.RA, MI-1, MI-2, MI-3] *Operational constraints* due to the loss or compromise of the PNT services or components are *understood and communicated* before continuing operations. [RS.AN-08] *Alert user community* of supply chain disruptions and threats describing the limitations and extent	*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. [RC.RP-01]

Example Scenarios	Govern	Identify	Protect	Detect	Respond	Recover
					of the threat in PNT source *integrity and availability.* [RS.CO-02, RS.CO-03]	

2076