Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date February 11, 2021

Original Release Date October 22, 2020

Superseding Document

Status	Final
Series/Number	NIST Interagency or Internal Report 8323
Title	Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services
Publication Date	February 2021
DOI	https://doi.org/10.6028/NIST.IR.8323
CSRC URL	https://csrc.nist.gov/publications/detail/nistir/8323/final
Additional Information	https://www.nist.gov/pnt

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

Draft NISTIR 8323

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

Authors will be identified in the final version of the Profile.

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

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

Draft NISTIR 8323

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

Authors will be identified in the final version of the Profile.

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

October 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8323
88 pages (October 2020)

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

Public comment period: *October 22, 2020* through *November 23, 2020*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: mailto: pnt-eo@list.nist.gov

Reports on Computer Systems Technology

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

Abstract

The national and economic security of the United States (US) is dependent upon the reliable functioning of critical infrastructure. Positioning, Navigation and Timing (PNT) services are widely deployed throughout the critical infrastructure. A disruption or manipulation of PNT services would have adverse impacts on much of the nation's critical infrastructure. In a government wide effort to mitigate these impacts, Executive Order (EO) 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation and Timing Services* was issued on February 12, 2020. The EO tasks various Federal agencies with specific actions to ensure the responsible use of PNT services. The National Institute of Standards and Technology (NIST) as part of the Department of Commerce (DoC), is required to produce a "Profile" to address the responsible use of PNT services. This document is a PNT Profile that is based on the Cybersecurity Framework. The PNT serves as the foundation for the broad and varied stakeholder community using PNT services. The primary focus of this Profile is Cybersecurity as it relates to the US critical infrastructure. Applicability of this Profile to various sectors and sub-sectors is assumed, however sector specific concerns are not formally addressed. The EO provides guidance concerning the roles of the Sector Specific Agencies (SSAs) in regard to the specific PNT communities they serve, from which further sector efforts are expected to develop based on the use of this foundational Profile.

Keywords

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

Call for Patent Claims

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

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

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

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

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

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

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

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

Executive Summary

An Executive Summary is not available in this Draft but will be provided in the final version of the Profile.

Table of Contents

186
187 **List of Appendices**

191
192 **List of Figures**

196
197 **List of Tables**

1 PNT Profile: Introduction

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

1.1 Purpose and Objectives

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

Use of the PNT Profile will help organizations to:

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

1.2 Scope

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

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

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

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

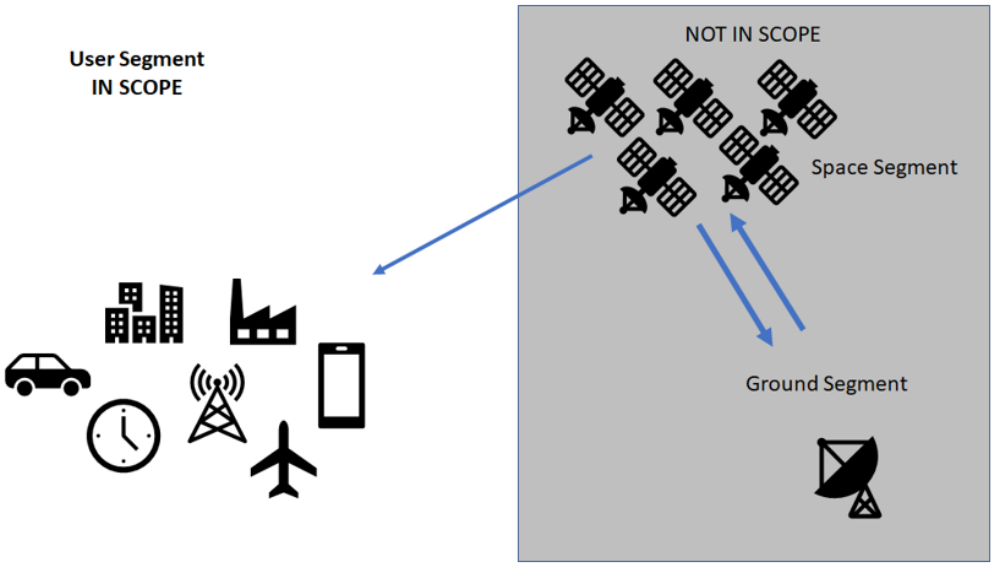

Figure 1- PNT User Segment Scope

This PNT Profile is limited to the user segment only. The provider (in this example, the GPS space and ground segments) is not part of this Profile.

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 cybersecurity risk management for systems that use PNT services;
- Procurement officials responsible for the 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 (hereafter, the Profile) is intended for a general audience and is broadly applicable. The Profile applies to organizations that:

- Have already adopted the NIST Cybersecurity Framework (CSF) to help identify, assess, and manage cybersecurity risks [NIST CSF];

- Are familiar with the CSF and want to improve their cybersecurity postures; or
- Are unfamiliar with the CSF but need to implement cybersecurity risk management frameworks for the responsible use of their PNT services.

2 Use the PNT Profile

The PNT Profile is a flexible tool that can be used in diverse ways by an organization to help meet mission and business objectives that are dependent upon the use of PNT services. An organization can use the PNT Profile in conjunction with its systematic process for identifying, assessing, and managing cybersecurity risk. The Profile can also help organizations determine cybersecurity risks based on their assessments of the potential impacts of manipulation or the disruption of PNT services to business and operational objectives. The Profile is intended to help users of PNT services prioritize necessary cybersecurity activities based on business objectives. Additionally, the Profile can be used to help organizations identify areas where standards, practices, and other guidance could help manage cybersecurity risks to systems that use PNT services.

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

- What processes and assets require PNT data (direct recipient of PNT services)?
- What processes and assets are dependent on other assets that require PNT data (i.e. identify secondary effects?)
- What processes and assets are vulnerable to disruption or manipulation of PNT services?
- 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 PNT Profile: 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 ensure resiliency. For example, a critical infrastructure may architect their distribution networks with multiple, independent PNT sources, communication paths, and communication mediums.

The Profile provides a starting point from which organizations can customize their approach and develop the most appropriate processes to manage cybersecurity risk to their PNT services and data essential for the reliable and efficient behavior of critical infrastructure applications.

Organizations can use the PNT Profile in conjunction with existing cybersecurity risk management processes. The PNT Profile assumes that the organization implements cybersecurity risk management processes for critical infrastructure, and this profile is intended to cover additional cybersecurity risk management processes specific to PNT. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO) 31000:2018, ISO/International Electrotechnical Commission (IEC) 27005:2018, and NIST Special Publication 800-39. A list of additional resources is included in Annex C of the PNT Profile.

3.2 Cybersecurity Framework Overview

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

The Cybersecurity Framework consists of three main components:

The Framework Core[1].

[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

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

The Core presents standards, guidelines, and practices within five concurrent and continuous Functions which are described below.

1. Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational to the effective use of the Cybersecurity Framework, enabling an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
2. Protect – Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impact of a potential cybersecurity event.
3. Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable the timely discovery of cybersecurity events.
4. Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity event.
5. Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impact of a cybersecurity event.

When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying Categories and Subcategories for each Function. The 108 Subcategories are the discrete cybersecurity outcomes that are organized into 23 Categories like "Asset Management" or "Protective Technology." **Table 1** shows the 5 Functions and 23 Categories of the Core.

[2] The word "outcomes" is used because the Cybersecurity Framework focuses on the "what" not 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 Informative References described on page 8 help organizations with the "how."

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

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection

			Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Informative References—such as existing standards, guidelines, and practices—provide practical suggestions for how to achieve the desired outcome of each Subcategory. An example of two Subcategories and, applicable Informative References, within the Supply Chain Risk Management Category are shown **Figure 2**.

Figure 2-Cybersecurity Framework Subcategory Example

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

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

Figure 3 shows how a custom-tailored profile can be built from the foundational PNT "Core" Profile in section 3.3. The tailored profile can be built using as inputs the business objectives, threat environment and requirements and controls. The outcomes associated with a custom profile based on the PNT profile are the outcomes from the Executive Order: the identification of systems dependent on PNT services that identify appropriate PNT service, detect disruption and manipulation of PNT services and managing the risk to those systems.

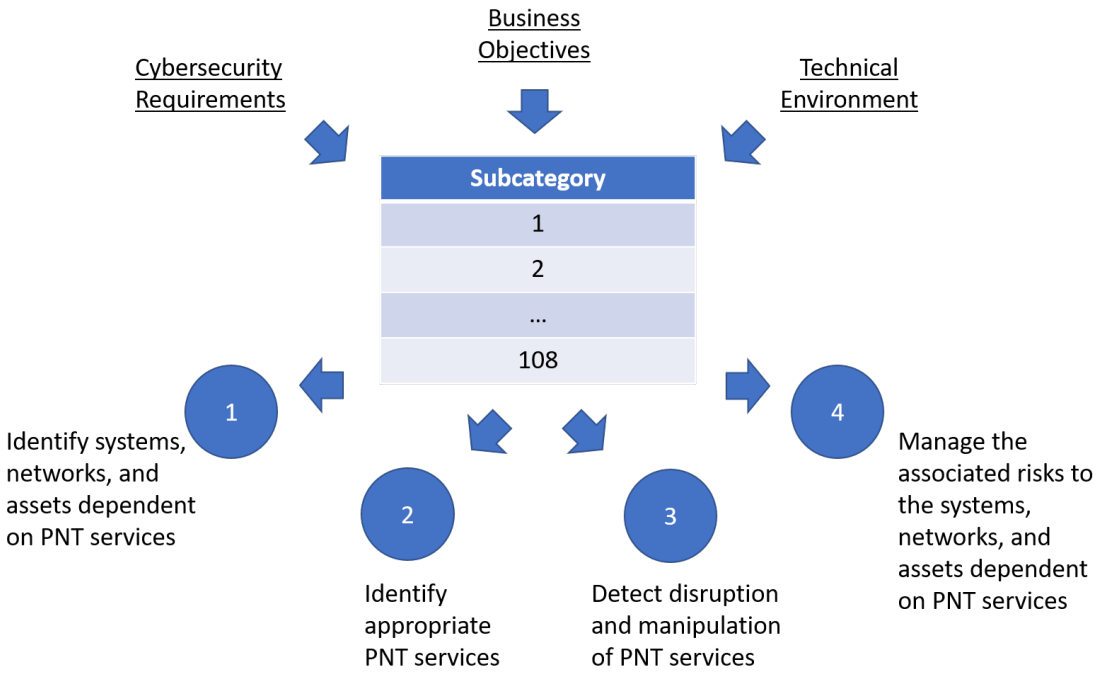

Figure 3-PNT Profile Creation Process

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

This profile is intended to be implemented within the larger context of an organization that is developing and executing its own robust cybersecurity program.[3] That program should be based on organizational cybersecurity risk management policies and procedures. This PNT profile is best implemented if the following programs and policies, identified below, are in place at the organizational level. However, this caveat does not preclude any organization from implementing the Profile should none of the below programs be in place.

- Cybersecurity program
- Business continuity plan
- Recovery plan

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

- Cybersecurity policy
- Cybersecurity plans
- Incident response plans

4 The PNT Profile

This section is organized in a manner that is consistent with the Cybersecurity Framework as described in Section 3.2. The tables summarize the subcategories for a function and a category. The informative references provided in the tables are PNT-specific and correspond to the subcategory but may not necessarily apply to all sectors.

The categories and subcategories defined by the Cybersecurity Framework will address different aspects of the four components identified in the Executive Order as illustrated in **Table** 2. Sections 4.1 through 4.6 will provide insight on how the sub-categories address the responsible use of PNT.

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

		Identify Systems dependent on PNT Services	Identify appropriate PNT Sources	Detect disturbance and manipulation of PNT services	Manage the risk to these systems
IDENTIFY	ASSET MANAGEMENT	X	X	X	X
	BUSINESS ENVIRONMENT	X	X	X	X
	GOVERNANCE	X			
	RISK ASSESSMENT	X	X	X	X
	SUPPLY CHAIN RISK MANAGEMENT	X		X	X
PROTECT	ACCESS CONTROL	X	X	X	X
	AWARENESS AND TRAINING	X			
	DATA SECURITY	X	X	X	X
	INFORMATION PROTECTION PROCESSES AND PROCEDURES	X	X		X
	MAINTENANCE	X	X	X	X
	PROTECTIVE TECHNOLOGY		X	X	X
DETECT	ANOMALIES AND EVENTS	X		X	X
	SECURITY CONTINUOUS MONITORING	X	X	X	X

	DETECTION PROCESS	X		X	X
RESPOND	RESPONSE PLANNING				X
	COMMUNICATIONS	X			X
	ANALYSIS			X	X
	MITIGATION			X	X
	IMPROVEMENTS				X
RECOVER	RECOVERY PLANNING	X		X	X
	IMPROVEMENTS	X		X	X
	COMMUNICATIONS	X		X	X

The Executive Order defines four components and the CSF defines a set of functions and categories. The Profile maps the components of the Executive Order to the CSF. It is important to note that there are interdependencies between the CSF functions and that each component of the Executive Order will require multiple functions, categories and subcategories.

Successful implementations require a holistic approach rather than a checklist.

4.1 Identify Function

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

4.1.1 Asset Management Category

The data, personnel, devices, systems, and facilities that enable the organization to achieve its business objectives must be identified and managed in a manner that is consistent with their

relative importance to organizational objectives and the organization's risk strategy. In the context of this profile, the assets that require PNT services in order to fulfill its purpose are identified.

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

457

Table 3-Identify – Asset Management Sub-Categories Applicable to PNT

Identify **Asset Management**		
Subcategory	**Applicability to PNT**	**References (PNT-Specific)**
AM-1: Physical devices and systems within the organization are inventoried	Document and maintain an inventory of the PNT system components that reflect the current system. PNT system components may include GPS/GNSS receivers, radio navigation or timing antennas, network switches, IoT/SCADA devices, and NTP and PTP servers. Identify all ports that send or receive PNT data, as well as the physical input/output interfaces, protocol versions and configuration options, for all devices that form or use PNT data to ensure compatibility. The calibration of component delays (e.g., antenna, surge suppressors, cables, connectors, splitters, receivers, switches, etc.) should be recorded to optimize the absolute accuracy and/or relative precision in deploying systems that form and use PNT data. Delay variations and the stability of each component due to temperature or aging, should be characterized in the environment in which the PNT system will be deployed.	**CISA** 1.a, 2.a **DHS GPS CI** **IEEE 1588** Annex N.1.2 **IMO 1575 C.1** **ITU-T GNSS** 2 **NIST SP 800-53 Rev. 4** CM-8, CM-9 PM-5 **NIST SP 250-29** **USG FRP**

	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. Particularly for applications that require traceability, document procedures for minimum periodic calibrations to a reference; after hardware updates, including FPGA code and firmware updates; and as part of the incident recovery plan. The frequency of calibrations is dependent on factors such as environmental conditions and PNT data performance requirements. Continuous time and frequency calibration services to UTC are also available. The physical inventory should include artifacts such as calibration procedures, configuration instructions and backups, architecture and wiring diagrams, and other documentation so that the reliance on and interdependency of PNT-related assets are understood at a system level. Use antennas to find PNT receivers when	

	doing physical inspections.	
AM-2: Software platforms and applications within the organization are inventoried	Document and maintain an inventory of PNT system software components that reflects the current system. PNT system software components may include, software license information, software version numbers, HMI and other ICS component applications, software, and operating systems. System software inventory is reviewed and updated as defined by the organization. For each software that provisions or uses PNT data, identify the input and output data interfaces; operating system environment; software maintenance procedures; configuration parameters, including default values and ranges; test plans; test result analysis; and other pertinent information to ensure consistent and valid deployments. Identify all software, applications, and systems that are dependent on PNT data. This recommendation includes software that relies on distributed time, using phase and frequency synchronization methods, including packet-based communication protocols (NTP, PTP) or physical signals (10 MHz, 1 PPS, IRIG-B),such as test and	**CISA** 1.b, 1.c **GPS-SPS-2020** B.1.2. **IEEE 2030.101** 4.4-4.7 **IMO 593**(13) **IMO 1575** B, C.1, E.1-E.3 **NIST SP 800-53 Rev. 4** CM-8, PM-5

	measurement tools, kernels, databases, logging software, cryptography/certificate management, and other applications that rely on synchronized clocks to ensure consistency. Identify the PNT data performance (accuracy, integrity) and resilience (continuity, availability, coverage) requirements for the software, applications, systems, and environment in which the system is operating. *Recognize that different users and applications may have different requirements.* Identify whether time synchronization and position tracking require absolute or relative accuracy and precision. Applications that require only knowledge of relative time, have additional possibilities for maintaining resilience using local sensors, computations, and communications.	
AM-3: **Organizational communication and data flows are mapped.**	Identify all connections within the PNT system as well as, between the PNT system and other systems. All connections are documented, authorized, and reviewed. Connection information may include, the physical interface characteristics, data characteristics, ports, protocols, addresses,	**CISA 1.b, 2.a** **IMO 1575** **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8

	description of the data, security requirements, and nature of the connection. Identify the PNT data source and distribution medium for the applications and systems that meets the PNT data performance and resilience requirements needed. It is critical to know where each system derives PNT data from. For example, the organization may want to investigate software programs that can help its organization identify your PNT data sources in an effort to assess which sources are most beneficial to organizational mission stability. Identify methods to resolve PNT data discrepancies among PNT sources.	
AM-4: **External information systems are catalogued.**	Identify and document all external connections for the PNT system. Examples of external systems include engineering design services, and those that are controlled under separate authority, personal devices, and other hosted services. Incorporate a configuration management tool that locates where all PNT antennas. Identify all PNT data sources and related	**CISA** 3.b **GPS ICD-870** 3.1. **IMO 1575** **NIST SP 800-53 Rev. 4** AC-20, SA-9 **USG FRP** Appendix B

	data products that pertain to an event or the status of the PNT source.	
AM-5: **Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.**	Identify and prioritize PNT system components and functions based on their classification, criticality, and business value. Identify the types of information in the organization's possession, custody, or control for which security safeguards are needed (e.g., sensitive or protected information). 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. Identify a PNT architecture to support the resources that require varying levels of PNT data integrity based on accuracy and associated statistical confidence parameters, including timeliness of detection, response and recovery.	**DHS PNT** **DOT 12464** **IEC 61850-90-4 Part 10** **IEC 61850-90-4 Part 14** **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6

458

4.1.2 Business Environment Category

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

There are two subcategories within Identify Business Environment that apply to the PNT profile, as summarized in the table below.

Table 4-Business Environment Subcategories Applicable to PNT

Identify **Business Environment**		
Subcategory	Applicability to PNT	References (PNT-Specific)
BE-4: Dependencies and critical functions for delivery of critical services are established.	Identify and prioritize supporting services for critical PNT system processes and components. Identify and prioritize internal critical business services that are dependent on PNT system processes and components. For organizations that form PNT data, understand PNT data performance, the resilience levels of the service provided, and customer dependencies on PNT data.	**CISA** 3.a, 3.b, 3.c **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14 **USG FRP** 4, 6A
BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Identify PNT data resilience requirements and, whether PNT data is of critical services. Performance parameters may include availability and uncertainty of PNT data relative to ground truth and may require PNT systems that provide continuity. Record absolute or relative PNT data error	**CISA** 1.f, 6.a, 6.b, 6.c **DHS PNT** **DHS RCF** **GPS-SPS-2020** A.5.4.1 **IETF 8633**

	tolerances that, serve as detection thresholds, which can be expressed as a statistical distribution and within the confidence levels needed for operations. Identify requirements on notification/alarm communication time upon nearing and exceeding thresholds. Different applications can have different requirements. Requirements should be considered and prioritized in the context of safety, operational criticality, cost and other resource availability. Where applicable and practical, identify network performance parameters at the device's ingress and egress ports, static and dynamic link delays between nodes, and end-to-end communications for the distribution of PNT data. Infrequent events, such as leap seconds, may be handled differently by different sources of PNT. End users should understand how these events and their implementations impact operations. Identify performance levels of PNT data regardless of environmental threats or if applications can rely on alternatives without the PNT data (systems/components). Identify mitigation strategies to temporary PNT disruptions for all critical services. 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.	**IMO 1575** C.22, E.4 **Kaplan 2017** Chapters 9-13 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14 **USG FRP** 1.7.2 **Volpe 2001** 4

	Ensure the ability to maintain business continuity during events that impact organizational mission status through the practice of leveraging alternate timing service sources based on system priority classifications. Identify all possible failure modes and fault 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. Identify diverse, complementary PNT sources with an understanding of benefits, limitations and dissimilar failure modes to increase the probability that the PNT service is able to detect anomalous inputs and remain available through the presence of different threat models. Evaluate PNT services based on organizational requirements and risks. Evaluation criteria for PNT data source and communications architecture can include: system accuracy, system precision, system integrity, system reliability, system availability, communications security, spectrum availability, signal coverage, received signal strength, signal propagation, signal continuity, signal acquisition and tracking continuity, multipath effects, noise effects, susceptibility to natural or man-made disruption (e.g., radio frequency interference [RFI], susceptibility to cyber threats (e.g., supply chain vulnerabilities, environmental effects), platform dynamics, human factors engineering, and requirements for	

	installation and operation (e.g., service provider and user equipment cost, computing, space, weight, and power considerations). For the failure analysis, identify effects on the PNT data, means of detection and managing temporary disruptions, and effects on the applications that are dependent on the PNT data. Manage the residual risk of PNT disruptions through personnel training, additional sensors, and available data.	

4.1.3 Governance Category

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

There is one subcategory within Identify Governance that applies to the PNT profile.

Table 5-Governance Subcategory Applicable to PNT

Identify **Governance**		
Subcategory	Applicability to PNT	References (PNT-Specific)
GV-4: Governance and risk management processes address cybersecurity risks	Develop a comprehensive strategy to manage risk to PNT operations. Include cybersecurity considerations in the risk management strategy. Review and update the risk management strategy, as necessary.	**CISA** 2.b, 3.a **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM9, PM-10, PM-11

	Determine and allocate required resources to protect the PNT system(s). Understand legal governance and oversight of PNT sources and applications/systems using PNT data for critical applications with respect to traceability, performance monitoring and resilience requirements. Understand standards that support interoperability for PNT services and national/international coordination to support performance, standardization, and cost minimization of user equipment.	**USG FRP** 1.7.5 through 1.7.9

4.1.4 Risk Assessment Category

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. In the context of this profile, the risk to the organizational operations in the event of a loss or degradation of PNT services. As an organization analyzes its mission objectives as they relate to reliance on or use of PNT data, there are a series of guiding questions that inform the process. They include:

- What are the threats to achieving mission objectives?
- What damages can result when those mission objectives are disrupted?
- What are the most important assets for a given mission objective?
- Where would a cyber event present a risk to the physical infrastructure?

There are five subcategories within Identify Risk Assessment that apply to the PNT profile, as summarized in the table below.

485

Table 6-Risk Assessment Subcategories Applicable to PNT

Identify **Risk Assessment**		
Subcategory	**Applicability to PNT**	**References (PNT-Specific)**
RA-1: Asset vulnerabilities are identified and documented.	Identify, document, and report vulnerabilities that exist on the PNT system and the system distributing PNT data. Where safe and feasible, include the use of vulnerability scanning on the PNT system, its components, or a representative system.	**CISA** 4.a **NTP SEC** **DHS GPS CI** **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 **NTP SEC** **USG FRP** 1.7.3
RA-2: Cyber threat intelligence is received from information sharing forums and sources.	Establish and maintain ongoing contact with security groups and associations and 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 threat awareness program that includes a cross-organization information-sharing capability. Organizations should consider having both an unclassified and classified information-sharing capability.	**CISA** 4.a **ICS-CERT** **NCCIC** **NERC EISAC** **NTP SEC** **NIST SP 800-53 Rev. 4** PM-15, PM-16 **USG FRP** Appendix B

RA-3: Threats, both internal and external, are identified and documented.	Conduct and document periodic assessment of risk to PNT systems that considers threats and the likelihood of impact to PNT operations and assets. The risk assessment includes threats from insiders (intended or inadvertent/unwitting), external parties, user errors, hardware malfunction, software error or vulnerability, transient network disturbances, environmental conditions (e.g., multipath, atmospheric scintillations, interference from other legitimate RF signals, foliage, temperature, aging, vibrations, power outages), legitimate or illegitimate RF interference (e.g., jamming and spoofing), network security compromises (e.g., denial of-service and delay attacks), and privacy concerns. Identify and characterize PNT error sources and error components to understand tolerance to threats and impacts. For example, time error is defined as the offset between the application device time and a reference time. Because clocks are imperfect, time is 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, changes in the network topology. Errors in signal regeneration or, analog to digital conversion, can contribute to time reference, time distribution, and user or application performance degradation.	**DOT 12464** **IETF 7384** 3.1-3.3 **IETF 8633** **IETF 8915** 8, 9 **IETF CMP** 6 **ITU-T 810** 4, 5 **ITU-T GNSS** Appendix II, V, VII **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM16 **NIST TN 1366**
RA-4: Potential business impacts and likelihoods are identified.	Identify the potential business impacts of an outage of PNT services. The likelihood of a PNT risk may also be empirically evaluated in a test or field environment. The impact of the threat on PNT data performance and resilience may be evaluated in a test or field environment. Consider the impact of both observed	**DOT 12464** **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM9, PM-11 **USG FRP** 1.7.3, E.4

	and anticipated threats on downstream applications and users, as well as the potential interval of time during which the threat can continue. For each identified threat, include the extent of impact, error manifestation (step or ramp error and rate of ramp), detection thresholds, and error propagation implications on safety and operations.	
RA-5: **Threats, vulnerabilities, likelihoods, and impacts are used to assess risk.**	The organization's failure and fault analysis should include all threats to business processes due to an outage of PNT services. Understand the vulnerabilities of the PNT service given the operational environment. Estimate the internal and external, environmental, intentional, unintentional risk feasibility of the business or mission based on threats and the impact of a PNT outage.	**IETF 7384** 3.1-3.3 **IETF CMP** **IMO 1575** E.4 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16

4.1.5 Supply Chain Risk Management Category

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

There is one subcategory within Identify Supply Chain Risk Management that applies to the PNT profile, as summarized in the table below.

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

Identify **Supply Chain Risk Management**		
Subcategory	**Applicability to PNT**	**References (PNT Specific)**
SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	Identify any external systems or services that the organization uses for ingesting PNT data. Identify any external systems or services that the organization is dependent on for its PNT data. Identify any consumers that rely on the organizations PNT data. Sound software assurance principles, access control capabilities, the ability to return to a known good state, and the ability to be updated and adaptable to new features and protections should be applied to all components of the PNT system.	**DHS GPS CI** 5 **DHS RCF** **NIST SP 800-53** Rev. 4 PM-9, RA-2, RA-3, SA-12, SA14, SA-15

495

496 ## 4.2 Protect Function

497 The Protect Function defines six categories, all of which have at least one subcategory that applies to the PNT profile to varying
498 degrees as summarized in Sections 4.2.1 through 4.2.6.

499 ### 4.2.1 Access Control Category

500 Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed
501 consistent with the assessed risk of unauthorized access to authorized activities. In the context of this profile, assets may include GNSS
502 antennas, receivers, servers, subscriptions etc. and "physical access" may include radio frequency emanations.

503 There are seven subcategories within Protect Access Control that apply to the PNT profile, as summarized in the table below.

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

Protect **Access Control**		
Subcategory	Applicability to PNT	References (PNT-Specific)
AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.	Establish and manage identification mechanisms and credentials for users and the PNT system. This subcategory is a prerequisite. Enable approved access lists for all controls that follow, NTP and PTP time servers, and other PNT systems. Establish and manage identification and authentication credentials of PNT data sources and applications using PNT data. End device implementations that receive PNT data can ensure that the data has been produced by a trusted identity and has not been modified without knowledge.	**DHS GPS CI** 1 **IEEE 1588** Annex P **IETF 7384** 5.1.1-5.1.5 **IETF 8573** **IETF 8915** 1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
AC-2: Physical access to assets is managed and protected.	Protect physical access to the PNT equipment and resources. 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,	**NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9.

	escort requirements, guards, fences, turnstiles, locks, and monitoring of facility access. For example, obscure the visibility of antennas from public access.	
AC-3: Remote access is managed.	Establish usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the systems that use or form PNT data. Consider radio frequency as part of remote access and employ appropriate mitigations at the receiving antennae. Remote access methods may include, wireless, dial-up, broadband, VPN connections, mobile device connections, and communications through external networks. Enable secure remote access and management to PNT systems and devices. Compliance to secure standardized network management protocols can facilitate remote network management and monitoring. Ensure the safe use of service and management protocols by following security alerts and adhering to latest best practices. Document the use of security capabilities such as access control lists and authentication as well as configuration parameters to reduce the probability of cyberattacks.	**IETF CMP** **IEEE 1588** P.2.5.3 **IEC 61850-90-12** **NENA 911** **NIST SP 800-53** Rev. 4, AC-18, AC-19, AC-20 **SNMP3** **SNMPSEC**
AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Create access control lists that enforce which authenticated users are authorized to use or perform actions on PNT systems. 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	**IEEE 1588** Annex P **IETF 7384** 5.1.3 **IETF 8915** 1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC5, AC-6, AC-14, AC-16, AC-24, SC-2, SC-3, SC-4

	identification or authentication (e.g., during emergencies).	
AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	Protect the network integrity of the systems that use PNT data by incorporating network segmentation and segregation where appropriate and compatible with those technologies. Identify and control connections between system components. Monitor and control connections and communications at the external boundary and at key internal boundaries data. Boundary protection mechanisms may include, boundary clocks, routers, gateways, unidirectional gateways, data diodes, and separating system components into logically separate networks or subnetworks.	**CISA** 4.a **IEEE 1588** Annex P **IETF 7384** 5.2 **NIST SP 800-53 Rev. 4** AC-4, SC-7
AC-6: Identities are proofed and bound to credentials and asserted in interactions.	PNT data sources are validated for authenticity. Clients, applications, and systems are validated for the authorized use of PNT data.	**CISA** 2.d **DHS GPS CI** **IEEE 1588** 16.14, Annex P **IETF 7384** 5.1.1-5.1.3 **IETF 8915** 1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security	Ensure that PNT devices and equipment use appropriate authentication for the risk associated with downstream operations which depend on accurate and reliable PNT data. Not all PNT services support authentication and alternates should be sought when practical and warranted.	**IEEE 1588** 16.14, Appendix P.2.1.2.2 **IETF 8915** 1,4, 5.5, 8.3, 8.4 **IETF 4082**

and privacy risks and other organizational risks).	During the time of calibration and initial turn on of a receiver, monitor the RF environment. Extra care needs to be taken when initially turning on a receiver. Where organizational policies require source authentication, a receiver of PNT data can authenticate the source of the data, ensure data provenance, and verify the integrity of the data. Users, devices, and assets are authenticated to prevent cyberthreats by remote users to the PNT data source.	

505

506 ### 4.2.2 Awareness and Training Category

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

510 There is one subcategory (Awareness and Training) that applies to the PNT profile.

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

Protect **Awareness and Training**		
Subcategory	Applicability to PNT	References (PNT-Specific)
AT-2: Privileged users understand their roles and	Ensure that users with privileged access to the PNT system(s) understand their requirements and responsibilities.	**CISA** 5.a, 7.a **NIST SP 800-53 Rev. 4** AT-3, PM-13

responsibilities	Determine how to establish what privileged user qualifications are, what training is required to meet qualifications, and ways to validate that the qualifications have been met. Operators, network/system administrators, and other technical staff are trained to install, test and maintain PNT systems as well as to detect, and respond to compromised PNT data with respect to the PNT data source and applications/systems using PNT data.	

512

513 ### 4.2.3 Data Security Category

514 Information and data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and
515 availability of PNT services. In this profile, availability and integrity of PNT services are of primary concern throughout the
516 enterprise. PNT data that is bound or associated with PII or other sensitive data increases the confidentiality concerns.

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

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

Protect **Data Security**		
Subcategory	Applicability to PNT	References (PNT-Specific)
DS-1: Data-at-rest is protected.	Use authoritative sources of PNT data products, such as informational almanacs and status information, with authentication and data integrity verification capabilities. Applications dependent on PNT data, such as location	**GPS ICD-870** 3.3, 3.3.1 **IETF CMP** 6 **NENA 911** 5

	and timestamp 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 host servers, users and devices may have important information used to alter information or other cyberthreats that can degrade the performance of the PNT service. Maintaining strict access control lists and, leveraging encryption are methods that can help protect the data at rest.	
DS-2: Data-in-transit is protected.	Use encryption and transmission security when available systems require authentication, integrity or confidentiality protections. Time protocols may need integrity, authentication, and for certain use cases confidentiality protections. Prior to deploying encryption/decryption schemes, validate the cryptographic algorithm and implementation's effect on delay asymmetries and that the synchronization precision remains within the permitted statistical tolerance. Establish and manage the identification and authentication credentials of PNT data sources and applications using PNT data.	**IEEE 1588** 16.14, Annex P.2.2.1.3, P.2.2.3 **IETF 7384** 5.2-5.3 **IETF NTS** 1-10.1, 10.2, **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12,
DS-3: Assets are formally managed throughout removal, transfers, and disposition.	Depending on the assessment of the sensitivity of PNT data, enforce accountability for all PNT system components throughout the system lifecycle, including removal, transfers, and disposition. Some of these Subcategory requirements can be met by implementing solutions that provide the hardware inventory, software inventory, systems development lifecycle management, and media sanitization technical capabilities.	**CISA** 4.6 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16

DS-4: Adequate capacity to ensure availability is maintained	Ensure that adequate resources (e.g., backup and complimentary sources) are maintained for PNT system information processing, networking, telecommunications, and data storage. Provide sufficient capacity to ensure availability and, stability, and minimize delay to meet application requirements within acceptable statistical tolerance. A robust network architecture can reduce the impact of PNT source and network attacks. Consider the redundant and diverse use of time sources and paths that can protect against and support detection of other time source corruption. Keep apprised of potential and scheduled disruptions from PNT service providers.	**IEEE 1588** Appendix P.2.3 **IETF 7384** 5.4 **NIST SP 800-53** Rev. 4 AU-4, CP-2, SC-5 **USG FRP** 1.7.5.2
DS-5: Protections against data leaks are implemented.	Protect the PNT system against data leaks. Special attention must be paid to PNT data which is used in conjunction with other data such as personal identifiable information (PII). The physical location of critical assets needs to be protected against data leaks.	**IEEE 1588** Annex J **IETF 8915** 1, 9,9.1 **IETF 8633** **IETF CMP** **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4,
DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	Changes in PNT firmware and software can be rolled back to the last known good state and should comply with the latest standards. Qualify new PNT firmware and software by verifying, validating, and executing documented device and end-to-end test plans under normal and failure mode conditions. Consider including potential PNT data interoperability issues in the affected application systems validation test plan, including	**CISA** 2.c **DHS GPS CI** 3 **DHS ST** **GPS IS-200** **GPS ICD-240** **GPS ICD-870**

	leap second and GPS week rollover testing, well in advance of an event. Information integrity may be checked or verified through the use of redundant or independent PNT sources. Methods to evaluate PNT data integrity include algorithms to: check the consistency of PNT output data and estimate the current magnitude and characteristics PNT data errors and uncertainty. End device implementations that receive PNT data can ensure that the data has been produced by a trusted identity and has not been modified without knowledge.	**IEEE 2030.101** 5 **IETF 8633** **IETF 8915** 1 5, 5.6, **IMO 1575** **NIST SP 800-53 Rev. 4** SC-16, SI-7
DS-8: Integrity checking mechanisms are used to verify hardware integrity.	Verify PNT device calibration, status, orientation (e.g., antenna positioning), and actual state compared to the desired state. Ensure adequate backup power is provided.	**DHS GPS CI** **IEEE 1588** M.4.2, M.4.3, N **NISTIR 8250** Appendix A **NIST SP 800-53 Rev. 4** PE-11, SA-10, SI-7

4.2.4 Information Protection Processes and Procedures Category

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

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

527

Table 11-Information Protection Processes and Procedures Applicable to PNT

Protect **Information Protection Processes and Procedures**		
Subcategory	Applicability to PNT	References (PNT-Specific)
IP-1: A baseline configuration of information technology / industrial control systems is created and maintained that incorporates security principles (e.g. concept of least functionality).	Characterize baseline PNT performance requirements and capabilities, such as error, wander and jitter bounds. Document baseline configurations for PNT devices and components(e.g. software license information, software version numbers, HMI and other ICS component applications, software, operating systems), current version numbers, patch information on operating systems and applications, configuration settings and parameters, network topology, and the logical placement of those components within the system architecture. 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. Install PNT devices and components using established safety and best practices guidelines. Verify that PNT devices and installation can meet performance requirements within statistical tolerance bounds. Configure the PNT devices and components to provide only essential capabilities. Review the baseline configuration and disable unnecessary capabilities.	**CISA** 4.b, 5.b **DHS GPS CI** **IEEE 1588** Annex P **IMO 1575** C.1 **ITU G. 8272** I.1 **ITU-T G.8275** **ITU-T GNSS** 4, 5, Appendix V, VII **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM5, CM-6, CM-7, CM-9, SA-10 **NTP SEC**

	Methods to protect exposed PNT assets include, obscuring antennas, using decoy antennas, considering whether CRPA antennas to protect from interference and jamming would improve PNT service performance for the applications, and considering the delay stability is within pre-defined thresholds for precision timing applications. Backup solutions include complementary sources, redundant antennas, spaced sufficiently apart, and high stability oscillators. Network communication architectures and protocols can also impact recovery time in the event of a path or node failure.	
IP-2: A System Development Life Cycle to use PNT services. Manage systems is implemented.	An operational system development life cycle for PNT services is established to incorporate security measures throughout the lifecycle of PNT systems by concentrating on the architectures, requirements, approach, and assumptions to minimize privacy risks for systems that use PNT, thereby ensuring the confidentiality, integrity, and availability of services.	**CISA** 4.b **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
IP-3: Configuration change control processes are in place.	Employ configuration change control for the PNT devices and components. Conduct impact analyses. Identify and record the effects of impact on downstream applications, users, and downtime. Manage a PNT system that leverage an SDLC to maintain a functioning baseline and monitor all changes to validate impacts and integrity.	**IMO 1575** C.1 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
IP-9: Response plans (Incident Response and Business	Develop and maintain response and recovery plans that identify essential functions and associated contingency requirements and provide a roadmap	**DHS IDM** **DHS RCF**

Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	for implementing incident response. Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments, and contact information. Address maintaining essential functions despite system disruption, as well as the eventual restoration of the PNT devices and components. Include considerations for PNT source holdover and complementary PNT sources with dissimilar failure modes. Define the incident types, resources and management support needed to effectively maintain and mature the incident response and contingency capabilities. Assess threat preparedness by verifying incident response and recovery plans through periodic simulated cyber-attack exercises for PNT data.	**DHS ST** **IEC 61850-90-12** 5.8 **NIST JRES 120.017** **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP13, IR-7, IR-8, IR-9, PE-17 **NIST TN1366** **USG FRP**
IP-10: Response and recovery plans are tested.	PNT response and recovery plans are tested. Review the results to determine the efficiency and effectiveness of the plans, as well as the readiness to execute the plans. Regarding this profile, use the results of the tests to inform other CSF functions such as “detect”.	**DHS RCF** **DHS ST** **NERC GridEx** **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14

4.2.5 Maintenance Category

Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. IN the context of this profile, the systems and components of interest include GNSS receivers, antennas, modules, time servers etc. Both subcategories within the Maintenance category apply to the PNT profile as summarized in the table below.

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

Protect		
Maintenance		
Subcategory	Applicability to PNT	References (PNT-Specific)
MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	Schedule, perform, record , and review records of maintenance and repairs on PNT devices and components. Assess the impact of the maintenance and repair of the PNT devices and components on the end user's performance and adjust accordingly. Verify that the behavior of PNT devices and components is within acceptable bounds.	**CISA** 4.a **IEEE 2030.101** 6 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
MA.2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	Enforce approval requirements, control, and monitoring of remote maintenance activities. Employ the appropriate level of authentication, logging, record keeping, and session termination for remote maintenance.	**CISA** 4.b, **IEEE 1588** P.2.4 **IETF 8633** 3.1 **NIST SP 800-53 Rev. 4** MA-4

534

535 ### 4.2.6 Protective Technology Category

536 Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies,
537 procedures, and agreements. In the context of this profile, systems and assets that receive, transport or form data from PNT service
538 providers.

539 There are five subcategories within the Protective Technology category that apply to the PNT profile, as summarized in the table
540 below.

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

Protect **Protective Technology**		
Subcategory	Applicability to PNT	References (PNT-Specific)
PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	Generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or PNT components associated with the event. PNT-dependent applications that require an audit trail often require legal or metrological traceability, an unbroken documented chain of calibrations, from a trusted reference (e.g., UTC) to the end user. UTC(NIST) and UTC(USNO) are the sources of legal time in the U.S. As part of characterizing the physical device using or forming PNT data, determine the delay between the device clock and the timestamping functions used for the audit and logs.	**CISA** 7.a **IEEE 1588** 16.14.4.4.2 **Matsakis 2018** III, IV, V **NIST SP 800-53 Rev. 4** AU (all)
PT-2: Removable media is protected, and its use restricted according to policy.	Employ safeguards to restrict the use of portable media when used on PNT devices and components. Ensure that PNT devices and equipment follow organizational policy on removable media.	**NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP5, MP-7, MP-8
PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	PNT deployment should employ the principle of least functionality. Configure the PNT system to provide only essential capabilities.	**IEEE 1588** Annex P2.5.1,2.5.5 **IETF CMP** 6 **IETF 7384** 7.3

	When PNT data / services do not require functionality from intermediary nodes, they can be disabled to minimize attack surfaces.	**NIST SP 800-53 Rev. 4** AC-3, CM-7
PT-4: Communications and control networks are protected.	PNT systems have a high availability, integrity and stability requirement. Identify communications and control network requirements for availability, integrity, authentication, stability, confidentiality, and other pertinent parameters based on classes of applications. Ensure cyber hygiene in communications and control networks. For example, some NTP/PTP devices have multiple network ports that could be configured to isolate control traffic. As needed, consider transport security for networks that distribute PNT data. However, careful thought and validation are needed for higher precision timing applications since cryptographic algorithms and implementations can lead to time synchronization performance degradation.	**IEEE 1588** 16.14.4.4.2, Annex P **ITU-T G.8275** **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC38, SC-39, SC-40, SC-41, SC-43,
PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	PNT mechanisms include measures such as redundant PNT sources, fused PNT sources, holdover thresholds, or others in accordance with the resiliency requirements of the mission.	**DHS RCF** 5.3-5.5 **IEEE 1588** 9.3, 16.4, 17 **NIST SP 800-53 Rev. 4 CP**-7, CP-8, CP-11, CP13, PL-8, SA-14, SC-6

4.3 Detect Function

The Detect Function within the Cybersecurity framework defines three categories, all of which have subcategories that apply to the PNT profile to varying degrees as summarized in Sections 4.3.1 through 4.3.3.

4.3.1 Anomalies and Events Category

Anomalous activity is detected, and the potential impact of events is understood. In the context of this profile, the detection of erratic PNT data or a loss of PNT data for some period. There are five subcategories within Detect Anomalies and Events that apply to the PNT profile as summarized in the table below.

Table 14-Anomalies and Events Subcategories Applicable to PNT

Detect **Anomalies and Events**		
Subcategory	Applicability to PNT	References (PNT-Specific)
AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	Ensure 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. In exchanging information on PNT data performance, where possible, comply with standards for data exchange and interoperability.	**CISA** 1.d **GPS ICD-870** 3.1 **IEEE 1588** Annex J **IETF CMP** **IMO 1575** D, D.1, D.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4 **USG FRP** Appendix B
AE-2: Detected events are analyzed to understand attack targets and methods.	Review and analyze detected events within the PNT system to ensure normalcy of operations. Be able to differentiate between potential cyber incidents and understand attack targets and methods. Be able to distinguish between and/or predict potentially harmful events and normal operations. Consider the PNT system when analyzing the	**DHS GPS CI** **Kaplan 2017** Chapters 9, 10 **NIST SP 800-53 Rev.** 4 AU-6, CA-7, IR-4, SI-4

	cybersecurity event. Preserve data for analysis and characterization of future disturbance events.	
AE-3: Event data are collected and correlated from multiple sources and sensors.	Ensure that event data is compiled across the PNT system using various sources such as event reports, logs, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Multiple sensors and sources can be used to correlate fault modes and contribute to anomaly detection models and algorithms. Network performance monitoring can provide an indication or signature of nominal behavior and be used to detect anomalies.	**GPS ICD-870** 3.1 **IEEE 1588** Annex J **IETF CMP** **Kaplan 2017** Chapters 12-13 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 **USG FRP** Appendix B
AE-4: Impact of events is determined	In the context of PNT, the impact of the event is a function of the operational phase of the enterprise and the environment. Both routine and anomalous PNT events 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. 4** CP-2, IR-4, RA-3, SI-4
AE-5: Incident alert thresholds are established	PNT incident thresholds established to indicate the potential impact to the mission are essential to ensuring that proper reporting and alerting thresholds are in place. Based on mission requirements, consider reviewing and revising thresholds on a continuous basis.	**DHS RCF** 3.2 **IMO 1575** 2.2.1, Appendix C **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8 **USG FRP** Appendix A

551

4.3.2 Security Continuous Monitoring Category

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

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

Table 15-Security Continuous Monitoring Subcategories Applicable to PNT

Detect **Security Continuous Monitoring**		
Subcategory	Applicability to PNT	References (PNT-Specific)
CM-1: The network is monitored to detect potential cybersecurity events.	Monitor the PNT source, distribution medium characteristics, and PNT data output, as well as additional characteristics from applications and systems dependent on PNT data for anomalous behavior. Heighten system monitoring activity whenever there is an indication of increased risk. Identify the monitoring strategy and determine acceptable performance thresholds of PNT data and other system behaviors for all identified fault modes. Monitoring thresholds can be determined from nominal and anomalous data for each fault mode. Consider relevant fault parameters and acceptance bounds based on reasonable or conservative criteria for various classes of applications and users.	**CISA** 1.d **DOT 12464** **IEEE 1588** 16.11, 16.12, J.1 through J.5, P.2.4 **IETF CMP** **ITU-T GNSS Appendix** III, V **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM3, SC-5, SC-7, SI-4 **USG FRP** Appendix B

	Detection models can leverage correlations between fault modes and minimum detectable limits. Analyze the threat model to determine if some faults can remain undetected, their impacts, and whether they pose an acceptable risk to the organization. Continue to improve the monitoring strategy as new fault modes are identified and until detection performance is acceptable.	
CM-2: The physical environment is monitored to detect potential cybersecurity events.	Physical access to PNT devices and components is actively monitored to detect potential breaches in security. Actively monitor the physical environment to include the RF environment. PNT devices and equipment may be located in remote locations. Physical access monitoring and controls should be chosen appropriately. Solutions that were implemented in use cases include electronic access control systems.	**DHS GPS CI** **IEC 61850-90-12** 7.12.4.12, 7.12.4.13 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
CM-3: Personnel activity is monitored to detect potential cybersecurity events.	The scope of the monitoring can include elements such as: native operating system/device capabilities, electronic access control systems, physical access control systems (e.g., sign in/out sheets, logging, etc.), security status monitoring of personnel activity associated with the PNT system(s), detecting software use and installation restrictions.	**IEC 61850-90-12** 7.12.4.12, 7.12.4.13 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
CM-4: Malicious code is detected.	Deploy malicious code detection mechanisms, such as behavioral anomaly detection tools, throughout the PNT system(s) where safe and feasible to detect and eradicate malicious code. Should a PNT data consumer experience an anomaly, consider investigating the PNT system. Systems that use and support PNT data should be	**CISA** 4.a **NIST SP 800-53 Rev. 4** SI-3, SI-8

	used in the antivirus analysis. Update malicious code protection mechanisms, such as antivirus protections, whenever new releases are available in accordance with the configuration management policy and procedures for the PNT system(s) involved.	
CM-5: Unauthorized mobile code is detected.	PNT devices and equipment contain operating systems and may be vulnerable to unauthorized mobile code introduced by other vectors. Robust unauthorized mobile code detection mechanisms are highly recommended because vulnerabilities may be inherited from other applications of the mobile code.	**CISA** 4.a **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
CM-6: External service provider activity is monitored to detect potential cybersecurity events.	Detect deviation from PNT service providers interface specifications, which are defined in a service level agreement (SLA) with the service provider. This can include signal integrity, availability, continuity, and coverage.	**GPS CMPS** **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	Conduct ongoing security status monitoring on PNT system(s) for unauthorized personnel, connections, devices, access points, and software. Monitor for system inventory discrepancies. It is highly recommended that the data collected from systems that use and support PNT is aggregated, correlated, and produces notable events.	**NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 **NTP MON**
CM-8: Vulnerability scans are performed.	Conduct vulnerability scans on PNT system(s) where safe and feasible. 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.	**CISA** 1.a **NIST SP 800-53 Rev. 4** RA-5 **NIST SP 800-115**

4.3.3 Detection Processes Category

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

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

Table 16-Detection Processes Applicable to PNT

Detect **Detection Processes**		
Subcategory	Applicability to PNT	References (PNT-Specific)
DP-1: Roles and responsibilities for detection are well-defined to ensure accountability.	Define roles and responsibilities for detection activities on PNT systems and ensure accountability.	**GPS CMPS** **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, **USG FRP** 2.1-2.4
DP-3: Detection processes are tested.	Validate that event detection processes are operating as intended. PNT devices and components that are upgraded are revalidated with end-to-end testing by the users. Perform periodic testing to verify the integrity of the detection process.	**DHS RCF** **DHS TEST** **NIST SP 800-53 Rev. 4** CA-2, CA-7
DP-4:	Communicate PNT event detection and PNT data quality to personnel, partners, analytics, and	**GPS-ICD-870E**

Event detection information is communicated.	downstream application users. When the cause of a PNT disruption event is suspected to be external, share event detection with the appropriate external stakeholders for further investigation.	**IEEE 1588** 7.6.2, 16.11, 16.12 **IETF CMP** **IMO 1575** 2.3, B.2.2.1 **ITU-T G.8275** **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA5, SI-4 **USG FRP** Appendix B
DP-5: Detection processes are continuously improved.	Periodically examine the organization's PNT event detection processes and seek to improve them continuously.	**DHS ST** **NIST SP 800-53 Rev. 4** CA-2, CA-5, CA-7, PL-2, PM-14, RA-5, SI-4

4.4 Respond Function

Develop and implement the appropriate activities to respond to a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impacts of a potential cybersecurity event.

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

4.4.1 Response Planning Category

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents

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

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

Respond **Response Planning**		
Subcategory	Applicability to PNT	References (PNT-Specific)
RP-1: Response plan is executed during or after an incident.	Execute the response plan during or after a cybersecurity event affecting PNT system(s) in accordance with the pre-defined threshold. Document response plans including categories of incidents and PNT resilience level requirements based on application criticality and impact.	**DHS RCF** **DHS ST** **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 **USG FRP**

575

576 ### 4.4.2 Communications Category

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

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

581

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

Respond **Communications**		
Subcategory	Applicability to PNT	References (PNT-Specific)
CO-1: Personnel know their roles and order of operations when a response is needed.	Ensure that personnel are trained to respond to PNT disruptions, 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.	**CISA** 1.f **IMO 1575** C.2.2 **NIST SP 800-61** **NIST SP 800-34 Rev.1** 3.2.1, CP-2, CP-3, IR-3, IR-8 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
CO-2: Incidents are reported consistent with established criteria.	Ensure that cybersecurity events on the PNT system are reported consistent with the response plan. Suspected intentional interference should be reported to the appropriate channels.	**NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8 **NIST SP 800-61 Rev. 2** 4 **DHS IDM** **NERC CIP-008-6** **NERC EISAC** **USG FRP**
CO-3: Information is shared consistent with response plans.	Share cybersecurity incident information with relevant stakeholders as defined in the organizational sharing policies.	**CISA** 1.d, 1.f **DHS IDM**

	Based on feasibility, include the ability of PNT systems and PNT data information sharing to alert downstream users and applications of performance degradation or loss of PNT data, allowing applications and users to respond in near real-time to the degradation based on application tolerances of PNT data loss and degradation.	**FCC** **IEEE 1588** 7.6.2, 16.11, 16.12 **IETF CMP** **NAVCEN** **NERC EISAC** **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 **NIST SP 800-61 Rev. 2** 2.4
CO-4: Coordination with stakeholders occurs consistent with response plans.	In the event of PNT disruption or manipulation, coordinate PNT cybersecurity incident response actions with all relevant stakeholders.	**DHS IDM** **NERC EISAC** **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 **NIST SP 800-61 Rev. 2** 2.4

4.4.3 Analysis Category

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

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

589

Table 19-Subcategories Applicable to PNT

Respond **Analysis**		
Subcategory	Applicability to PNT	References (PNT-Specific)
AN-1: Notifications from detection systems are investigated.	Investigate cybersecurity-related notifications generated from PNT anomaly detection systems. DHS coordinates the development, implementation, and exercise of procedures to enable federal agencies with assigned responsibilities, authorities, and jurisdictions to investigate and mitigate GPS-based PNT interference.	**DHS IDM** **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
AN-2: The impact of the incident is understood.	Understand the full implication of a cybersecurity incident based on thorough investigation and analysis results. Consider the organizational impact on PNT services that may affect downstream applications, users, and systems that are dependent on PNT. Understand the root cause and impacted downstream relationships through leveraging mapped services and outlined policies, as well as the scope and necessary actions required for remediation. Correlate detected event information and incident responses with risk assessment outcomes to achieve perspective on incident impacts across the organization.	**ITU-T G.8275.1**Annex D **NIST SP 800-53 Rev. 4** CP-2, IR-4 **NIST SP 800-61 Rev. 2** 3

AN-3: Forensics are performed.	Conduct forensic analysis on collected cybersecurity event information to determine the root cause of PNT disruption or manipulation.	**NIST SP 800-53 Rev. 4** AU-7, IR-4 **NIST SP 800-61 Rev. 2** 3
AN-4: Incidents are categorized consistent with response plans.	Categorize cybersecurity incidents according to the level of severity and impact consistent with the response plan.	**NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8 **NIST SP 800-61 Rev. 2** 2 3.2
AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers.)	For PNT components and applications 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 **GPS-ICD-240** **NCCIC** **NIST SP 800-53 Rev. 4** PM-15, SI-5 **NIST SP 800-61 Rev. 2** 3, 3.2 **NTP SEC** **USG FRP** Appendix B

4.4.4 Mitigation Category

Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. In the context of PNT, mitigate may include rollover to alternate PNT sources, notification of external stakeholders of ongoing PNT anomalies or other activities.

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

596

Table 20-Mitigation Subcategories Applicable to PNT

Respond **Mitigation**		
Subcategory	Applicability to PNT	References (PNT-Specific)
MI-1: Incidents are contained.	Containment of a PNT event may require notification of downstream users and the transition to alternate PNT source(s) in accordance with the business continuity plan for containment. Contain cybersecurity incidents to minimize impact on the PNT system. PNT systems can revert to a known good state.	**DHS GPS CI** 4 **NIST SP 800-53 Rev. 4** IR-4, IR-8 **NIST SP 800-61 Rev. 2** 3.4.1
MI-2: Incidents are mitigated.	Given successful containment measures, implement PNT-based mitigation measures that can include alternate sources in order to operate through the incident. Once the effects of the incident(s) are contained, steps to correct the system are taken. These steps include measures such as 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. Mitigation procedures or measures should be part of the business continuity plan.	**DHS IDM** **NIST SP 800-53 Rev. 4** IR-4, IR-8 **NIST SP 800-61 Rev. 2** 3.4 **NTP SEC**
MI-3: Newly identified vulnerabilities are mitigated or	Newly identified PNT vulnerabilities are mitigated or documented as acceptable risks.	**IMO 1575** C.2.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5

documented as accepted risks		**NIST SP 800-61 Rev. 2** 3 **NTP SEC**

597

598 ### 4.4.5 Improvements Category

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

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

Respond **Improvements**		
Subcategory	Applicability to PNT	References (PNT-Specific)
IM-1: Response plans incorporate lessons learned.	PNT response plans incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.	**NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 **NIST SP-800-61 Rev. 2**
IM-2: Response strategies are updated.	Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned. Update the response plans to address changes to the organization, PNT system, attack vectors, environment of operation and problems encountered during plan implementation, execution, and testing. Updates may include, responses to disruptions or manipulations, as well as predetermined procedures. Update PNT disruption event characterization	**DHS IDM** **DOT 12464** **IMO 1575** E.1 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 **NTP SEC**

	documentation as well as organization or industry shared databases to track the observed probability of occurrence in order to continuously update the risk assessment and response plans. Analyze the impact of the PNT anomaly on user and application errors. Characterize statistics based on nominal and anomalous PNT data. Response timeliness and prioritization based on application criticality are key to reducing impacts. 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.	

4.5 Recover Function

Develop and implement the appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impacts of a cybersecurity event.

The Recover Function within the Cybersecurity Framework defines three categories. Other than identify appropriate PNT sources" all of these categories and subcategories correlate with all of the components of the EO.

4.5.1 Recovery Planning Category

Recovery processes and procedures are executed and maintained to ensure the restoration of systems or assets affected by cybersecurity incidents.

There is one subcategory within Response Planning that applies to the PNT profile.

613

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

Recover **Recovery Planning**		
Subcategory	Applicability to PNT	References (PNT-Specific)
RP-1: Recovery plan is executed during or after a cybersecurity incident.	The business continuity plan should include a recovery plan. Execute the recovery plan during or after a cybersecurity incident on the PNT system. 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. Perform system acceptance testing. The recovery plan can include specific actions for restoration, recalibration and resetting of equipment.	**NIST SP 800-34 Rev. 1** **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8 **NIST SP 800-184**

615

616 ### 4.5.2 Improvements Category

617 Recovery planning and processes are improved by incorporating lessons learned into future activities. In the context of this profile, the
618 efficacy of the response actions such as notification and rollover are evaluated and improved should a similar event occur.

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

620

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

Recover **Improvements**		
Subcategory	Applicability to PNT	References (PNT-Specific)
IM-1: Recovery plans incorporate lessons learned.	PNT recovery plans incorporate lessons learned from ongoing incident handling activities into incident recovery procedures, training, and testing and implement the resulting changes accordingly. Consider creating and developing a database to archive all incidents and identify new fault modes and effects in order to facilitate analysis, including correlations, probability and location of fault modes. Data and resulting analysis can be used in the future identification of risks and preventative actions as well as the development of monitoring, detection, response, and recovery features. Common data formats, when agreed upon between stakeholders, facilitate information sharing to strengthen the protection of the user community.	**DOT 12464** **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 **NIST SP 800-61 Rev. 2** 3.4 **NTP SEC**
IM-2: Recovery strategies are updated.	Enable a process for the recovery plan to evolve to reflect new threats, improved technology, and lessons learned. Updates may include, recovery from disruptions or manipulations, and predetermined procedures. Update the recovery plan to address changes to the organization, PNT system, environment of operation and problems encountered during plan implementation, execution, and testing. Recovery timeliness and prioritization based on	**NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 **NIST SP 800-61 Rev. 2** 3.4

	application criticality are key to reducing impacts.	

4.5.3 Communications Category

Restoration activities are coordinated with internal and external parties. In the context of this profile, external parties may include industry associations that provide insight with respect to how PNT service was restored after events such as PNT interference, corrections for anomalies etc.

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

Table 24-Communications Subcategories Applicable to PNT

Recover **Communications**		
Subcategory	Applicability to PNT	References (PNT-Specific)
CO-1: Public relations are managed.	Centralize and coordinate information distribution and manage the public-facing representation of the organization. Public relations management may include, managing media interactions, creating privacy policies, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and e-mail requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of the information provided to the media, and ensuring personnel are familiar with public relations.	**NIST SP 800-34 Rev. 2** 4 **NIST SP 800-53 Rev. 4** IR-4 **NIST SP 800-184** 2.4
CO-2:	Employ a crisis response strategy to protect against negative impact and repair organizational	**NIST SP 800-53 Rev. 4** IR-4 **NIST SP 800-184** (all sections)

Reputation is repaired after an incident.	reputation. Crisis response strategies may include, actions to shape attributions of the crisis, change perceptions of the organization in crisis, and reduce the negative effect generated by the crisis.	
CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	Communicate recovery activities to all relevant internal and external stakeholders, executive teams, and management teams.	**DOT 12464** **DHS ST** **NIST SP 800-34 Rev. 2** **NIST SP 800-53 Rev. 4** CP-2, IR-4 **NIST SP 800-184** **NTP SEC**

629

5 Conclusion

A Conclusion is not available in this Draft but will be provided in the final version of the Profile.

References

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

[DHS GPS CI] Department of Homeland Security. Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure. (DHS, Washington, DC). https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf

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

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

[DHS RCF] Department of Homeland Security (2020) Resilient PNT Conformance F Framework, DRAFT. (DHS, Washington, DC).

[DHS ST] 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 TEST] Department of Homeland Security (2020) GPS Equipment Testing for Critical Infrastructure. (DHS, Washington, DC). Available at: https://beta.sam.gov/opp/d3489175b4544508acdae10f91769b7b/view

[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). https://rosap.ntl.bts.gov/view/dot/12464/dot_12464_DS1.pdf

[EO 13636] Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013.

https://www.govinfo.gov/content/pkg/FR-2013-02-

19/pdf/2013-03915.pdf

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

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

[GPS ICD-240] GPS.gov (2020) *GPS ICD 240C Navstar GPS Control Segment to User Support Community.* (National Coordination Office for Space-Based Positioning, Navigation, and Timing, Washington, DC). https://www.gps.gov/technical/icwg/ICD-GPS-240C.pdf

[GPS ICD-870] GPS.gov (2020) *GPS ICD 870E NAVSTAR Next Generation GPS Control Segment (OCX) to User Support Community Interface*. (National Coordination Office for Space-Based Positioning, Navigation, and Timing, Washington, DC). https://www.gps.gov/technical/icwg/ICD-GPS-870E.pdf

[GPS IS-200] GPS.gov (2020) *IS-GPS-200L NAVSTAR GPS Space Segment/Navigation User Segment Interfaces*. (National Coordination Office for Space-Based Positioning, Navigation, and Timing, Washington, DC). https://www.gps.gov/technical/icwg/IS-GPS-200L.pdf

[GPS CMPS] GPS.gov (2020) U.S. Global Positioning System (GPS) Civil Monitoring Performance Specification (CMPS). (National Coordination Office for Space-Based Positioning, Navigation, and Timing, Washington, DC). https://www.gps.gov/technical/ps/2020-civil-monitoring-performance-specification.pdf

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

[GPS SPS-2020] GPS.gov (2020) *U.S. Global Positioning System (GPS) Standard Positioning Service (SPS) Performance Standard*, 5th Edition. (National Coordination Office for Space-Based Positioning, Navigation, and Timing, Washington, DC). https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf

[ICS-CERT] Cybersecurity & Infrastructure Security Agency (2020) Industrial Control

Systems. (DHS, Washington, DC). Available at: https://us-cert.cisa.gov/ics

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

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

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

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

[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. 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. https://tools.ietf.org/html/rfc8573

[IETF 8633] Reilley 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. https://tools.ietf.org/html/rfc8633

[IETF 8915] Franke D, Sibold D, Danserie M, Sunblad R, Teichel K (2020) Using the Network Time Security Specification to Secure the Network Time Protocol. (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 88915.

https://tools.ietf.org/html/rfc8915

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

[IETF NTS] Franke D, Sibold D, Teichel K, Dansarie M, Sundblad R (2020) Network Time Security for the Network Time Protocol Internet Engineering Task Force (IETF) Network Time Protocol Working Group). https://tools.ietf.org/html/draft-ietf-ntp-using-nts-for-ntp-28

[IMO 593] International Maritime Organization (1986) IMO 593(14) Accuracy Standards for Navigation. (IMO, London, England). http://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Assembly/Documents/A.593(14).pdf

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

[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).

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

[ITU-T G.8275.1] International Telecommunications Union Telecommunications Standardization Sector (2020) ITU-T G.8275.1/Y.1369.1 *Precision Time Protocol Telecom Profile for Phase/Time Synchronization with Full Timing Support from The Network.* (ITU-T, Geneva, Switzerland). Available at: https://www.itu.int/rec/T-REC-G.8275.1/en

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

[Kaplan 2017] Kaplan E, Hegarty C. (2006). *Understanding GPS: principles and applications.* (Artech House, Boston MA). 2nd ed.

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

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

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

[NENA 911] National Emergency Number Association (2019) *NENA 01-023 NENA i3 Standard for Next Generation 9-1-1,* DRAFT. (NENA, Alexandria, VA). Available at: https://dev.nena.org/higherlogic/ws/public/download/16133/STA-010.3 i3 Standard PubRev.pdf

[NERC CIP-008-6] North American Electric Reliability Corporation (2020) *CIP-008-6 Cyber Security Incident Reporting and Response Planning.* 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

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

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

[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. http://dx.doi.org/10.6028/jres.120.017

[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

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

[NIST SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1 [NIST SP 800-34]

[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 (2013) 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. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

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

[NIST SP 800-82] 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

[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 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: https://nvlpubs.nist.gov/nistpubs/Legacy/TN/nbstechnicalnote1366.pdf

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

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

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

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

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

[USG FRP] Department of Defense, Department of Homeland Security, and Department of Transportation (2019) 2019 Federal Radionavigation Plan (National Technical Information Service, Springfield, Virginia) DOT-VNTSC-OST-R-15-01. https://www.navcen.uscg.gov/pdf/FederalRadioNavigationPlan2019.pdf

[VIM] Bureau International des Poids et Mesures, 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. https://www.bipm.org/en/publications/guides/#vim

[Volpe 2001] Volpe JA (2001) Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System Final Report. U.S. Department of Transportation, Washington DC). https://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf

Appendix A—Acronyms and Abbreviations

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

Term	Definition
CISA	Cybersecurity and Infrastructure Security Agency
CRPA	Controlled Reception Patterned Antenna
CSF	Cybersecurity Framework
DHS	Department of Homeland Security
DOT	Department of Transportation
EISAC	Electricity Information Sharing and Analysis Center
EO	Executive Order
FCC	Federal Communications Commission
FPGA	Field-programmable Gate Array
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HMI	Human Machine Interface
ICS	Industrial Control System
IDM	Interference Detection and Mitigation
IEC	International Eletrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMO	International Maritime Organization
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
ITU-T	International Telecommunications Sector
NAVCEN	U.S. Coast Guard Navigation Center
NCCIC	National Cybersecurity and Communications Integration Center
NERC	North American Electric Reliability Corporation
NGS	National Geodetic Survey
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NTP SEC	NTP Security Notice

Term	Definition
PII	Personally Identifiable Information
PNT	Positioning, Navigation and Timing
PNT Profile	The PNT Responsible Use Cybersecurity Framework Profile
PPS	Pulse per second
PTP	Precision Time Protocol
RF	Radio Frequency
RFC	Request for Comments
RFI	Radio Frequency Interference
RTO	Recovery Time Objectives
SCADA	Supervisory Control and Data Acquisition
SP	Special Publication
UE	User Equipment
USG FRP	US Government Federal Radionavigation Plan
USNO	United States Naval Observatory
UTC	Coordinated Universal Time
VPN	Virtual Private Network

914

Appendix B—Glossary

Selected terms used in in this document are defined below.

Accuracy: (Absolute, Geodetic or Geographic accuracy). The accuracy of a position estimate with respect to the geographic or geodetic co-ordinates of the Earth. [IMO 915]

Accuracy (Absolute): The degree of conformity of a measured or calculated value

Allan deviation: A non-classical statistic used to estimate stability. This statistic is sometimes called the Allan variance, but since it is the square root of the variance, its proper name is the Allan deviation. The NIST-equation for the Allan deviation (with non-overlapping samples) is

$$\sigma_y(\tau) = \sqrt{\frac{1}{2(M-1)}\sum_{i=1}^{M-1}(\overline{y_{i+1}} - \overline{y_i})^2}$$

where $y_i$is a set of frequency offset measurements that consists of individual measurements, y_1, y_2, y_3, and so on; M is the number of values in the y_i series, and the data are equally spaced in segments τ seconds long. Or

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

where x_i is a series of phase 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 segments τ seconds long. [NIST Time and Frequency Glossary]

Atomic Clock: A clock referenced to an atomic oscillator. Only clocks with an internal atomic oscillator qualify as atomic clocks. [NIST Time and Frequency Glossary]

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

The principle underlying the atomic oscillator is that since all atoms of a specific element are identical, they should produce exactly the same frequency when they absorb or release energy. In theory, the atom is a perfect "pendulum" whose oscillations are counted to measure 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 Time and Frequency Glossary]

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. [Adapted from [USG FRP Appendix E]

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. [NIST Time and Frequency Glossary]

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 Time and Frequency 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 Time and Frequency Glossary]

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 a user will be able to determine a PVT solution within specified absolute or relative uncertainty and is able to monitor the integrity of the determined solution over the duration of an operation, presuming that the 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 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]

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

The apparent change of frequency caused by the motion of the frequency source (transmitter) relative to the destination (receiver). If the distance between the transmitter and receiver is increasing the frequency apparently decreases. If the distance between the transmitter and receiver is decreasing, the frequency apparently increases. To illustrate this, listen to the sound of

a train whistle as a train comes closer to you (the pitch gets higher), or as it moves further away (the pitch gets lower). As you do so, keep in mind that the frequency of the sound produced at the source has not changed. [NIST Time and Frequency Glossary]

Drift (frequency): The linear (first order) component of a systematic change in frequency of an oscillator over time. Drift is caused by aging, by changes in the environment, and by other factors external to the oscillator. [NIST Time and Frequency Glossary]

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 Time and Frequency 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 Time and Frequency 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 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 Time and Frequency 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 Time and Frequency 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, we can estimate frequency offset 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 Time and Frequency Glossary]

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, others have good long-term stability. Stability doesn't tell us 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 a number of similar statistics are also used. [NIST Time and Frequency Glossary]

Global Navigation Satellite System (GNSS): GNSS refers collectively to the world-wide positioning, navigation, and timing (PNT) determination capability available from one or more satellite constellations. Each GNSS system employs a constellation of satellites operating in conjunction with a network of ground stations. [USG FRP]

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

Holdover: An operating condition of a clock which has lost its controlling reference input and 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: Integrity is the 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.

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

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

Jitter: The abrupt and unwanted variations of one or more signal characteristics, such as the interval between successive pulses, the amplitude of successive cycles, or the frequency or phase of successive cycles. Although widely used in fields such as telecommunications, the term jitter is seldom used in time and frequency metrology, since terms such as phase noise are more descriptive. [NIST Time and Frequency Glossary]

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.

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]

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 Time and Frequency 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 primary used for time and frequency measurements are quartz oscillators and atomic oscillators. [NIST Time and Frequency Glossary]

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 Time and Frequency Glossary]

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

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

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: The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring. [NIST SP 800-30]

Risk Assessment: The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. [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 risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters. [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 Time and Frequency Glossary]

Stability: An inherent characteristic of an oscillator that determines how well it can produce the same frequency over a given time interval. Stability doesn't indicate whether the frequency is right or wrong, but only whether it stays the same. The stability of an oscillator doesn't necessarily change when the frequency offset changes. You can adjust an oscillator and move its frequency 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, 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 Time and Frequency Glossary]

Synchronization: The process of setting two or more clocks to the same time.

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 Time and Frequency 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, and 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 Time and Frequency Glossary]

Appendix C—Additional Resources

Additional Resources are not available in this Draft but will be provided in the final version of the Profile.