

2

3 **Foundational PNT Profile:**

4 **Applying the Cybersecurity Framework**

5 **for the Responsible Use of Positioning,**

6 **Navigation, and Timing (PNT) Services**

7

8 Initial Public Draft

9

10 Michael Bartock

11 Joseph Brule

12 Ya-Shian Li-Baboud

13 Suzanne Lightman

14 James McCarthy

15 Karen Reczek

16 Doug Northrip

17 Arthur Scholz

18 Theresa Suloway

19

20

21 This publication is available free of charge from:

22 <https://doi.org/10.6028/NIST.IR.8323r1.ipd>

27

28 **Foundational PNT Profile:**

29 **Applying the Cybersecurity Framework for the**

30 **Responsible Use of Positioning, Navigation, and**

31 **Timing (PNT) Services**

32 Initial Public Draft

33

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

Karen Reczek
*Standards Coordination
Office Laboratory Programs*

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

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

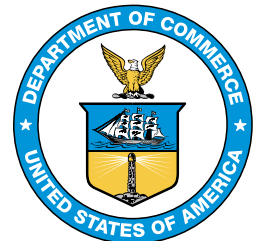
James McCarthy
*Applied Cybersecurity Division
Information Technology Laboratory*

34 This publication is available free of charge from:

35 <https://doi.org/10.6028/NIST.IR.8323r1.ipd>

36 June 2022

37



38 U.S. Department of Commerce

39 *Gina M. Raimondo, Secretary*

40 National Institute of Standards and Technology

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

42

43

44

45 National Institute of Standards and Technology Interagency or Internal Report 8323r1 ipd
46 Initial Public Draft
47 136 pages (June 2022)

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

50 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
51 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
52 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best
53 available for the purpose.

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

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

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

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

65 National Institute of Standards and Technology
66 Attn: Applied Cybersecurity Division, Information Technology Laboratory
67 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

68
69 All comments are subject to release under the Freedom of Information Act (FOIA).

70

71 **Reports on Computer Systems Technology**

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

80 **Abstract**

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

96 **Keywords**

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

99

Supplemental Content

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

103

Acknowledgments

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

107

Call for Patent Claims

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

114

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

117

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

120

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

124

125 i. under reasonable terms and conditions that are demonstrably free of any unfair
126 discrimination; or

127 ii. without compensation and under reasonable terms and conditions that are
128 demonstrably free of any unfair discrimination.

129

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

135

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

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

139 **Executive Summary**

140 Executive Order 13905, *Strengthening National Resilience Through Responsible Use of*
141 *Positioning, Navigation, and Timing (PNT) Services*, was issued on February 12, 2020 [EO
142 13905]. It seeks to protect the national and economic security of the United States from the
143 disruption or manipulation of systems that form or use PNT data and information vital to the
144 functioning of U.S. critical infrastructure and technology-based industries. The Executive Order
145 (EO) directs the Department of Commerce to develop a PNT Profile that will address the four
146 components of responsible use of PNT, as stated in the EO:

- 147 1. Identify systems that use or form PNT data.
- 148 2. Identify PNT data sources.
- 149 3. Detect disruption and manipulation of the
150 systems that form or use PNT services and
151 data.
- 152 4. Manage risk regarding responsible use of these systems.

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

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

169 **Table of Contents**

170 **Executive Summary vii**

171 **1 Introduction 1**

172 1.1 Purpose and Objectives 1

173 1.2 Scope 1

174 1.3 Audience 2

175 **2 Intended Use 4**

176 **3 Overview 5**

177 3.1 Risk Management Overview 5

178 3.2 Cybersecurity Framework Overview 5

179 **4 The PNT Profile 11**

180 4.1 Identify Function 14

181 4.1.1 Asset Management Category 14

182 4.1.2 Business Environment Category 20

183 4.1.3 Governance Category 23

184 4.1.4 Risk Assessment Category 24

185 4.1.5 Risk Management Strategy 30

186 4.1.6 Supply Chain Risk Management Category 32

187 4.2 Protect Function 34

188 4.2.1 Access Control Category 34

189 4.2.2 Awareness and Training Category 39

190 4.2.3 Data Security Category 41

191 4.2.4 Information Protection Processes and Procedures Category 46

192 4.2.5 Maintenance Category 53

193 4.2.6 Protective Technology Category 55

194 4.3 Detect Function 59

195 4.3.1 Anomalies and Events Category 60

196 4.3.2 Security Continuous Monitoring Category 63

197 4.3.3 Detection Processes Category 68

198 4.4 Respond Function 70

199 4.4.1 Response Planning Category 71

200 4.4.2 Communications Category 71

201 4.4.3 Analysis Category 74

202	4.4.4 Mitigation Category.....	76
203	4.4.5 Improvements Category	79
204	4.5 Recover Function.....	80
205	4.5.1 Recovery Planning Category.....	82
206	4.5.2 Improvements Category	83
207	4.5.3 Communications Category	84
208	References.....	86

209	List of Appendices	
210	Appendix A— Acronyms and Abbreviations	99
211	Appendix B— Glossary	101
212	Appendix C— Additional Resources	109
213	Appendix D— Applying the PNT Profile to Cybersecurity Risk Management	114
214	Appendix E— Organization Specific PNT Profiles	121

215	List of Figures	
216	Figure 1 - Example of How the PNT Profile Applies to GNSS.....	2
217	Figure 2 - Cybersecurity Framework Subcategory Example	9
218	Figure 3 - PNT Profile Creation Process	10
219	Figure 4 - Components of the PNT Profile	13

220	List of Tables	
221	Table 1 - Cybersecurity Framework Functions and Categories.....	7
222	Table 2 - Mapping the EO Implementation Guidance to the Cybersecurity Framework	
223	Profile.....	11
224	Table 3 - Identify – Asset Management Subcategories Applicable to PNT	15
225	Table 4 - Business Environment Subcategories Applicable to PNT	20
226	Table 5 - Governance Subcategory Applicable to PNT	23
227	Table 6 - Risk Assessment Subcategories Applicable to PNT	25
228	Table 7 - Supply Chain Risk Assessment Subcategory Applicable to PNT.....	32
229	Table 8 - Protect Access Control Categories Applicable to PNT	35
230	Table 9 - Awareness and Training Subcategory Applicable to PNT	40
231	Table 10 - Data Security Subcategories Applicable to PNT	41

232 Table 11 - Information Protection Processes and Procedures Applicable to PNT..... 47
233 Table 12 - Maintenance Subcategories Applicable to PNT 54
234 Table 13 - Protective Technology Subcategories Applicable to PNT 56
235 Table 14 - Anomalies and Events Subcategories Applicable to PNT 60
236 Table 15 - Security Continuous Monitoring Subcategories Applicable to PNT 63
237 Table 16 - Detection Processes Applicable to PNT..... 68
238 Table 17 - Response Planning Subcategory Applicable to PNT 71
239 Table 18 - Communications Subcategories Applicable to PNT 72
240 Table 19 - Subcategories Applicable to PNT..... 74
241 Table 20 - Mitigation Subcategories Applicable to PNT 77
242 Table 21 - Improvements Subcategories Applicable to PNT 79
243 Table 22 - Recovery Planning Subcategory Applicable to PNT 82
244 Table 23 - Improvements Subcategories Applicable to PNT 83
245 Table 24 - Communications Subcategories Applicable to PNT 85
246 Table 25 - Applying the PNT Profile to User Risk Management..... 115
247 Table 26 - Change Log..... 123
248

249 **1 Introduction**

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

256 **1.1 Purpose and Objectives**

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

263 Use of the PNT Profile will help organizations:

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

275 **1.2 Scope**

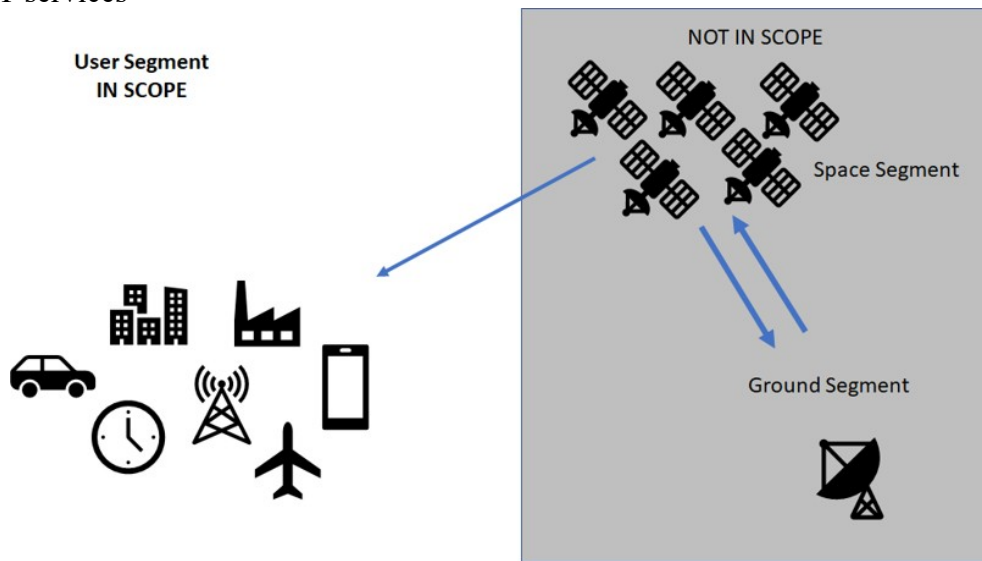
276 The PNT Profile's scope includes systems that use PNT services, including systems that consume and
277 then rebroadcast PNT data for consumption by other organizational entities where a PNT service is
278 defined as "any system, network, or capability that provides a reference to calculate or augment the
279 calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination
280 thereof" [EO 13905]. PNT service providers include government systems, such as Global Positioning
281 Systems (GPS), public NIST Network Time Protocol (NTP) servers, commercial services, and internal
282 systems. The PNT Profile's scope does not include source PNT signal generators and providers (e.g., a
283 Global Navigation Satellite System (GNSS) control segment or space segment, as shown in **Figure 1**).

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

288 realized, and manage the residual risk.

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

- 291 • Risk-informed management of PNT services;
- 292 • Risk-based approaches that minimize the potential effects
293 of the disruption or manipulation of PNT services and
294 data; and
- 295 • Deliberate planning and action regarding the secure management
296 of PNT services



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

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

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

304 **1.3 Audience**

305 This document's intended audience includes:

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

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

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

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

322 **2 Intended Use**

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

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

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

348 **3 Overview**

349 **3.1 Risk Management Overview**

350 Risk management is the ongoing process of identifying, assessing, and responding to risk as related to an
351 organization's mission objectives. To manage risk, organizations should understand the likelihood that
352 an event will occur as well as its potential impacts. An organization should also consider statutory and
353 policy requirements that may influence or inform cybersecurity decisions.

354 The PNT Profile supports and is informed by cybersecurity risk management processes. Using the PNT
355 Profile, organizations can make more informed decisions, based on business needs and risk assessments,
356 to select and prioritize cybersecurity activities and expenditures that help identify systems dependent on
357 PNT, identify appropriate PNT sources, detect disturbances and manipulation of PNT services, manage
358 the risk to these systems, and promote resiliency.

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

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

371 **3.2 Cybersecurity Framework Overview**

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

378 The NIST Cybersecurity Framework consists of three main components:¹

- 379 1. The Framework Core provides a catalog of desired cybersecurity activities and outcomes² using
380 common language. The Core guides organizations in managing and reducing their cybersecurity
381 risks in a way that complements an organization’s existing cybersecurity and risk management
382 processes.
- 383 2. The Framework Implementation Tiers provide context for how an organization views
384 cybersecurity risk management. The Tiers help organizations understand whether they have a
385 functioning and repeatable cybersecurity risk management process and the extent to which
386 cybersecurity risk management is integrated with broader organizational risk management
387 decisions.
- 388 3. The Framework Profiles are customized to the outcomes of the Core to align with an
389 organization’s requirements. Profiles are primarily used to identify and prioritize opportunities for
390 improving cybersecurity at an organization.

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

- 394 1. Identify: Develop the organizational understanding to manage cybersecurity risk to systems,
395 assets, data, and capabilities. The activities in the Identify function are foundational to the
396 effective use of the NIST Cybersecurity Framework, enabling an organization to focus and
397 prioritize its efforts in a manner consistent with its risk management strategy and business needs.
- 398 2. Protect: Develop and implement the appropriate safeguards to ensure the delivery of critical
399 infrastructure services. The activities in the Protect function support the ability to limit or contain
400 the impact of a potential PNT cybersecurity event.
- 401 3. Detect: Develop and implement the appropriate activities to identify the occurrence of a
402 cybersecurity event. The activities in the Detect function enable timely discovery of PNT
403 cybersecurity events.
- 404 4. Respond: Develop and implement the appropriate activities to take action regarding a detected
405 cybersecurity event. The activities in the Respond function support the ability to contain the
406 impact of a potential PNT cybersecurity event.
- 407 5. Recover: Develop and implement the appropriate activities to maintain plans for resilience and to
408 restore any capabilities or services that were impaired due to a cybersecurity event. The activities
409 in the Recover function support timely recovery to normal operations to reduce the impact of a
410 PNT cybersecurity event.

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

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

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

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

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

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

417

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

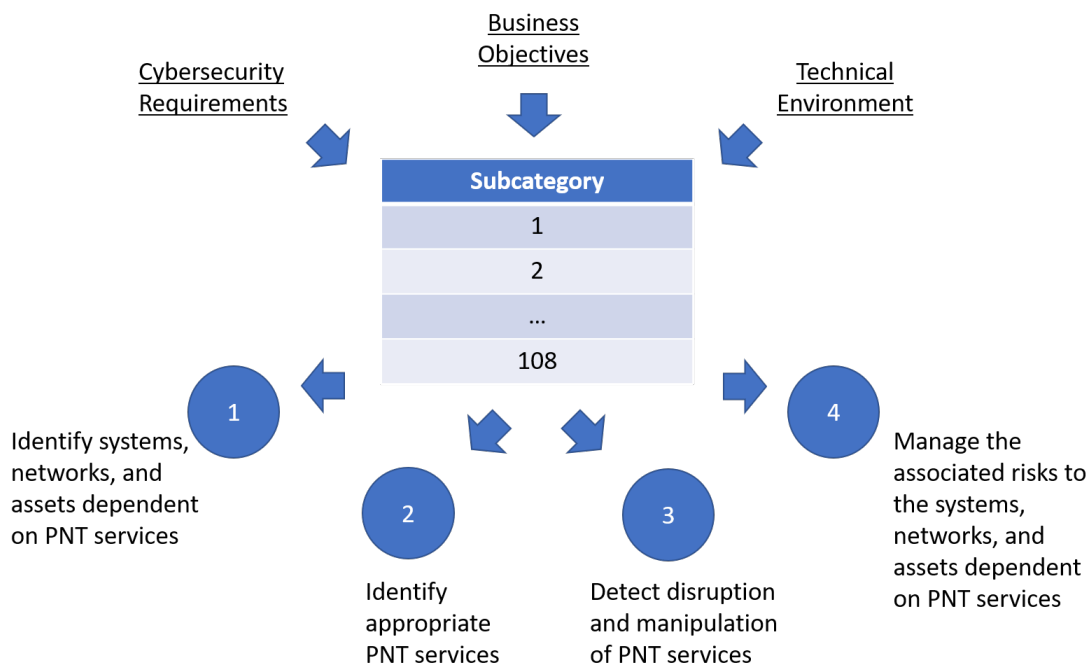
Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 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

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

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

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

434



435

Figure 3 - PNT Profile Creation Process

436 Since organizations within the PNT community sector or sub-sector share many of the same
 437 business objectives and regulatory requirements, the creation of a high-level profile can provide
 438 a common starting point. The PNT Profile can make it easier for organizations to begin
 439 incorporating cybersecurity and can also be used to provide a baseline of cybersecurity for
 440 organizations within a sector or sub-sector. Individual organizations can further customize a
 441 profile by taking the sector/sub-sector profile and then tailor or augment it to address
 442 requirements, business objectives, or environmental threats unique to them.
 443

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

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

450 **4 The PNT Profile**

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

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

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

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

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

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

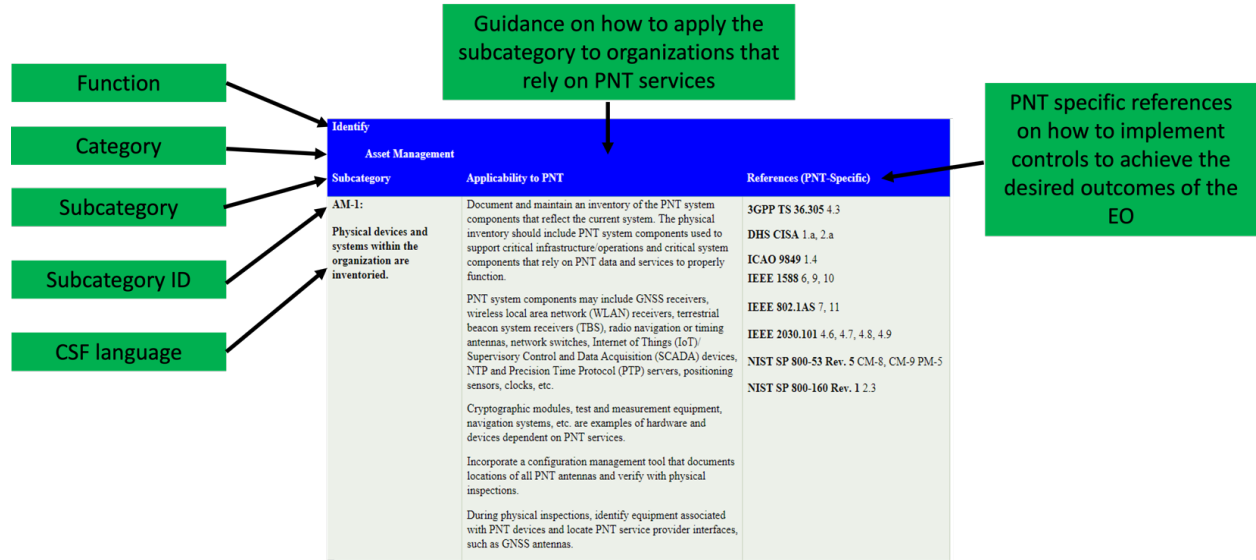


Figure 4 - Components of the PNT Profile

475

476 **4.1 Identify Function**

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

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

484 The objectives of the Identify function include:

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

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

493 **4.1.1 Asset Management Category**

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

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

Table 3 - Identify – Asset Management Subcategories Applicable to PNT

Identify		
Asset Management		
Subcategory	Applicability to PNT	References (PNT-Specific)
<p>AM-1:</p> <p>Physical devices and systems within the organization are inventoried.</p>	<p>Document and maintain an inventory of the PNT system components that reflect the current system. The physical inventory should include PNT system components used to support critical infrastructure/operations and critical system components that rely on PNT data and services to properly function.</p> <p>PNT system components may include GNSS receivers, wireless local area network (WLAN) receivers, terrestrial beacon system receivers (TBS), radio navigation or timing antennas, network switches, Internet of Things (IoT)/ Supervisory Control and Data Acquisition (SCADA) devices, NTP and Precision Time Protocol (PTP) servers, clocks, positioning sensors such as Inertial Navigation Systems (INS), Inertial Measurement Units (IMU), proximity sensors, etc.</p> <p>Cryptographic modules, test and measurement equipment, navigation systems, etc. are examples of hardware and devices dependent on PNT services.</p> <p>Incorporate a configuration management tool that documents locations of all PNT antennas and verify with physical inspections.</p>	<p>3GPP TS 36.305 4.3</p> <p>DHS CISA 1.a, 2.a</p> <p>ICAO 9849 1.4</p> <p>IEEE 1588 6, 9, 10</p> <p>IEEE 802.1AS 7, 11</p> <p>IEEE 2030.101 4.6, 4.7, 4.8, 4.9</p> <p>NIST SP 800-53 Rev. 5 CM-8, CM-9 PM-5</p> <p>NIST SP 800-160 Rev. 1 2.3</p>

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

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

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

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

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

502

503 **4.1.2 Business Environment Category**

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

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

509

Table 4 - Business Environment Subcategories Applicable to PNT

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

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

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

510 **4.1.3 Governance Category**

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

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

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

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

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

516 **4.1.4 Risk Assessment Category**

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

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

Table 6 - Risk Assessment Subcategories Applicable to PNT

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

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

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

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

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

522 **4.1.5 Risk Management Strategy**

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

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

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

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

528 **4.1.6 Supply Chain Risk Management Category**

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

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

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

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

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

535 **4.2 Protect Function**

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

540 The objectives of the Protect function include:

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

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

552 **4.2.1 Access Control Category**

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

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

Table 8 - Protect Access Control Categories Applicable to PNT

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

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

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

Protect		
Access Control		
Subcategory	Applicability to PNT	References (PNT-Specific)
	<p>Clients, applications, and systems are validated for the authorized use of the PNT data or services.</p> <p>Note that the sensitivity (and associated confidentiality requirements) of PNT data may be impacted when bound or associated with other data.</p>	<p>NIST SP 800-53 Rev. 5 AC-1, AC-2, AC-3, AC16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12,</p> <p>PE-2, PS-3</p>
<p>AC-7:</p> <p>Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).</p>	<p>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.</p> <p>Users, devices, and assets are authenticated to prevent the realization of cyberthreats via remote connections to the PNT data source.</p> <p>Authentication protects data provenance and verifies the authenticity of the data source. Implement source, client, or mutual authentication based on the IA requirements of the organization and be cognizant of the fact that different applications may have different authentication requirements.</p> <p>Understand that implementations may influence message delay and delay variations. Verify that PNT data performance remains within tolerances.</p>	<p>DHS CISA 2.d, 5.b</p> <p>DHS GPS CI</p> <p>DHS TFS 2.2</p> <p>IEEE 1588 16.14, Appendix P.2.1, 2.2</p> <p>IETF 4082 2-5</p> <p>IETF 5906 2-12</p> <p>IETF 7384 5.1, 5.7</p> <p>IETF 7822 2-4</p> <p>IETF 8573 3-7</p> <p>IETF 8633 5.5, 5.6</p> <p>IETF 8915 1,4, 5.5, 8.3, 8.4</p> <p>NIST NTP</p> <p>NIST SP 800-53 Rev. 5 AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11</p>

559 **4.2.2 Awareness and Training Category**

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

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

Table 9 - Awareness and Training Subcategory Applicable to PNT

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

566 **4.2.3 Data Security Category**

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

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

572 **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.	<p>Applications dependent on PNT data, such as location and time stamp to log the position and time of an event, may need to protect against repudiation and alteration. Sensitive information may need to be encrypted.</p> <p>PNT data may be critical for downstream activities, such as analytics and forensics. Apply measures such as access control lists, encryption, and other data-at-rest protections commensurate with the criticality of the activities dependent on PNT.</p>	<p>GPS ICD-870 3.3, 3.3.1 IETF CMP 6 NIST SP 800-37 3 NIST SP 800-53 Rev. 5 MP-3, MP-4, MP-6, SC-28</p>

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

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

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

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

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

573 **4.2.4 Information Protection Processes and Procedures Category**

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

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

Table 11 - Information Protection Processes and Procedures Applicable to PNT

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

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

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

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

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

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

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

581 **4.2.5 Maintenance Category**

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

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

Table 12 - Maintenance Subcategories Applicable to PNT

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

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

587 **4.2.6 Protective Technology Category**

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

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

591 the table below.

592

Table 13 - Protective Technology Subcategories Applicable to PNT

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

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

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

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

593 **4.3 Detect Function**

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

597 The objectives of the Detect function include:

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

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

602 **4.3.1 Anomalies and Events Category**

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

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

606 **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.	Verify that operational PNT data performance baselines and expected data flows for relevant external PNT information systems, the organization’s PNT system, and applications dependent on PNT data are captured, developed, and maintained to detect events. When practical, comply with standards-based solutions for data formatting, message formatting, and message transmission to facilitate interoperability and integration.	DHS 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. 5 AC-4, CA-3, CM-2, SC-16, SI-4 RTCA 229 1.5.2, 1.7.2 USG FRP Appendix B

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

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

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

607 **4.3.2 Security Continuous Monitoring Category**

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

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

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

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

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

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

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

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

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

615 **4.3.3 Detection Processes Category**

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

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

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

Detect		
Detection Processes		
Subcategory	Applicability to PNT	References (PNT-Specific)

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

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

621 **4.4 Respond Function**

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

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

628 The objectives of the Response function are to:

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

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

635 **4.4.1 Response Planning Category**

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

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

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

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

639 **4.4.2 Communications Category**

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

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

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

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

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

645 **4.4.3 Analysis Category**

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

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

649 **Table 19 - Subcategories Applicable to PNT**

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

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

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

650 **4.4.4 Mitigation Category**

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

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

Table 20 - Mitigation Subcategories Applicable to PNT

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

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

656 **4.4.5 Improvements Category**

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

660 **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. 5 CP-2, IR-4, IR-8 NIST SP-800-61 Rev. 2

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

661 **4.5 Recover Function**

662 The Recover function develops and implements the appropriate activities to maintain plans for resilience and restore any
663 capabilities or services that were impaired due to a cybersecurity event.

664 The activities in the Recover function support timely recovery to normal operations and return the organization back to its
665 proper working state after a disruption or manipulation of PNT services has occurred. The effectiveness of the Recover
666 function is dependent upon implementation of the previous functions—Identify, Protect, Detect, and Respond.

667 The objectives of the Recovery function are to:

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

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

673 **4.5.1 Recovery Planning Category**

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

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

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

Recover		
Recovery Planning		
Subcategory	Applicability to PNT	References (PNT-Specific)
<p>RP-1:</p> <p>Recovery plan is executed during or after a cybersecurity incident.</p>	<p>The business continuity plan should include a recovery plan. Execute the recovery plan during or after a cybersecurity incident on the PNT system.</p> <p>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.</p> <p>The recovery capability of the equipment, including devices that can operate through an incident, is part of a PNT system’s recovery process. Perform system acceptance testing.</p> <p>The recovery plan can include specific actions for restoration, recalibration, resetting, and test validation of equipment.</p>	<p>DHS RCF 5, 6</p> <p>ICAO 9849 7.7</p> <p>IEEE 2030.101 5</p> <p>NIST SP 800-34 Rev. 1</p> <p>NIST SP 800-53 Rev. 5 CP-10, IR-4, IR-8</p> <p>NIST SP 800-160 Rev. 1 3.4.11, Appendix F.2.6</p> <p>NIST SP 800-184</p> <p>RTCA 229 2.4, 2.5</p>

678 **4.5.2 Improvements Category**

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

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

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

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

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

684 **4.5.3 Communications Category**

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

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

689

Table 24 - Communications Subcategories Applicable to PNT

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

690

691 References

- 692 [3GPP TS22.071] 3rd Generation Partnership Project (2022) Location Services (LCS)
693 Service description Stage 1(Release 17) March 2022. (Technical
694 Specification Group Services and System Aspects, Sophia Antipolis,
695 France). Specification 22.071. Available at
696 [https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetail
697 s.aspx?specificationId=584](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=584)
- 698 [3GPP TR22.826] 3rd Generation Partnership Project (2021) Study on Communication
699 Services for Critical Medical Applications (Release 17.2) March 2021.
700 (Technical Specification Group Services and System Aspects, Sophia
701 Antipolis, France). Specification 22.826. Available at
702 [https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetail
703 s.aspx?specificationId=3546](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3546)
- 704 [3GPP TR22.878] 3rd Generation Partnership Project (2021); Feasibility Study on 5G
705 Timing Resiliency System (Release 18.2) December 2021. (Technical
706 Specification Group Services and System Aspects, Sophia Antipolis,
707 France). Specification TR.878. Available at
708 [https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetail
709 s.aspx?specificationId=3769](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3769)
- 710 [3GPP TS36.305] 3rd Generation Partnership Project (2022) Stage 2 functional
711 specification of User Equipment (UE) positioning in E-UTRAN
712 (Release 17) (Radio Access Network Evolved Universal Terrestrial
713 Radio Access Network (E- UTRAN,) March 2022. Specification
714 TS36.305. Available at
715 [https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetail
716 s.aspx?specificationId=2433](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2433)
- 717 [ATIS-I-0000070] ATIS-I-0000070 (2018) *Context-Aware Identity Management*
718 *Framework*. (ATIS, Washington, DC). Available at
719 [https://access.atis.org/apps/group_public/download.php/43565/ATIS-I-
720 0000070.pdf](https://access.atis.org/apps/group_public/download.php/43565/ATIS-I-0000070.pdf)
- 721 [Barret 2018] Barrett M (2018) *Framework for Improving Critical Infrastructure*
722 *Cybersecurity Version 1.1, NIST Cybersecurity Framework*. Available
723 at: <https://doi.org/10.6028/NIST.CSWP.04162018>
- 724 [BDS ICD] China Satellite Navigation Office (2019) *BeiDou Navigation Satellite*
725 *System Signal In Space Interface Control Document Open Service*
726 *Signal BII Version 3.0*.
- 727 [CNSSI 4009] Committee on National Security Systems (2015) *Committee on National*
728 *Security Systems Glossary*. Committee on National Security Systems
729 Instruction (CNSSI) No. 4009, April 2015. Available at

- 730 <https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf>
- 731 [DHS CISA] Cybersecurity & Infrastructure Security Agency (2020) Time Guidance
732 for Network Operators, Chief Information Officers, and Chief
733 Information Security Officers. (DHS, Washington, DC). Available at
734 [https://www.cisa.gov/sites/default/files/publications/time_guidance_netw](https://www.cisa.gov/sites/default/files/publications/time_guidance_network_operators_cios_cisos_508.pdf)
735 [ork_operators_cios_cisos_508.pdf](https://www.cisa.gov/sites/default/files/publications/time_guidance_network_operators_cios_cisos_508.pdf)
- 736 [DHS GPS CI] Department of Homeland Security. Improving the Operation and
737 Development of Global Positioning System (GPS) Equipment Used by
738 Critical Infrastructure. (DHS, Washington, DC). Available at
739 [https://www.cisa.gov/uscrt/sites/default/files/documents/Improving_the](https://www.cisa.gov/uscrt/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf)
740 [_Operation_and_Development_of_Global_Positioning_System_%28GP](https://www.cisa.gov/uscrt/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf)
741 [S%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf](https://www.cisa.gov/uscrt/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf)
- 742 [DHS IDM] Department of Homeland Security (2008) United States Positioning,
743 Navigation, and Timing Interference Detection and Mitigation Plan
744 ummary. (DHS, Washington, DC). Available at
745 <https://www.gps.gov/news/2008/2008-04-idm-public-summary.pdf>
- 746 [DHS PNT] Department of Homeland Security (2020) Report on Positioning,
747 Navigation, and Timing (PNT) Backup and Complementary
748 Capabilities to the Global Positioning System (GPS.) (DHS,
749 Washington, DC). Available at
750 [https://www.cisa.gov/sites/default/files/publications/report_on_pnt-](https://www.cisa.gov/sites/default/files/publications/report_on_pnt_backup_complementary_capabilities_to_gps_508.pdf)
751 [backup_complementary_capabilities_to_gps_508.pdf](https://www.cisa.gov/sites/default/files/publications/report_on_pnt_backup_complementary_capabilities_to_gps_508.pdf)
- 752 [DHS RCF] Department of Homeland Security (2022) Resilient PNT Conformance
753 Framework. (DHS, Washington, DC). Available at
754 [https://www.dhs.gov/sites/default/files/2022-](https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf)
755 [05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf](https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf)
- 756 [DHS S&T] Department of Homeland Security (2020) *Science and Technology*
757 *Position, Navigation, and Timing (PNT) Program*. (DHS, Washington,
758 DC). Available at [https://www.dhs.gov/science-and-technology/pnt-](https://www.dhs.gov/science-and-technology/pnt-program)
759 [program](https://www.dhs.gov/science-and-technology/pnt-program)
- 760 [DHS S&T 2022] Department of Homeland Security (2022) *Resilient Positioning,*
761 *Navigation, and Timing (PNT) Reference Architecture Version 1.0*.
762 (DHS, Washington, DC). Available at [https://www.dhs.gov/science-and-](https://www.dhs.gov/science-and-technology/publication/resilient-pnt-reference-architecture)
763 [technology/publication/resilient-pnt-reference-architecture](https://www.dhs.gov/science-and-technology/publication/resilient-pnt-reference-architecture)
- 764 [DHS TFS] Department of Homeland Security (2015) Best Practices for Improved
765 Robustness of Time and Frequency Sources in Fixed Locations. (DHS,
766 Washington, DC). Available at
767 [https://www.dhs.gov/sites/default/files/publications/GPS-PNT-Best-](https://www.dhs.gov/sites/default/files/publications/GPS-PNT-Best-Practices-Time-Frequency-Sources-Fixed-Locations-508.pdf)
768 [Practices-Time-Frequency-Sources-Fixed-Locations-508.pdf](https://www.dhs.gov/sites/default/files/publications/GPS-PNT-Best-Practices-Time-Frequency-Sources-Fixed-Locations-508.pdf)

- 769 [DIA] Defense Intelligence Agency (2022) DIA Challenges to Security in
770 Space. (DIA, Washington, DC). Available at
771 [https://www.dia.mil/Portals/110/Documents/News/Military_Power_Pub](https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf)
772 [lications/Challenges_Security_Space_2022.pdf](https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf)
- 773 [DOT] Department of Transportation. *What is Positioning, Navigation and*
774 *Timing (PNT)?* (Department of Transportation, Washington, DC).
775 Available at [https://www.transportation.gov/pnt/what-positioning-](https://www.transportation.gov/pnt/what-positioning-navigation-and-timing-pnt)
776 [navigation-and-timing-pnt](https://www.transportation.gov/pnt/what-positioning-navigation-and-timing-pnt)
- 777 [DOT CGSIC] Department of Transportation. (2020) *Civil GPS Service Interface*
778 *Committee*. (Department of Transportation, Washington, DC.) Available
779 at <https://www.gps.gov/cgsic/>
- 780 [DOT CMPS] Department of Transportation (2020) *Global Positioning System (GPS)*
781 *Civil Monitoring Performance Specification, 3rd Edition*. (Department of
782 Transportation, Washington, DC), GPS Civil Monitoring Performance
783 Specification DOT-VNTSC-FAA-20-08. Available at
784 [https://www.gps.gov/technical/ps/2020-civil-monitoring-performance-](https://www.gps.gov/technical/ps/2020-civil-monitoring-performance-specification.pdf)
785 [specification.pdf](https://www.gps.gov/technical/ps/2020-civil-monitoring-performance-specification.pdf)
- 786 [DOT 12464] Van Dyke K, Kovach K, Lavrakas J (2004) Status Update on GPS
787 Integrity Failure Modes and Effects Analysis. (Department of
788 Transportation, Washington, DC). Available at
789 https://rosap.ntl.bts.gov/view/dot/12464/dot_12464_DS1.pdf
- 790 [EO 13905] Executive Order 13905 (2020) Strengthening National Resilience
791 Through Responsible Use of Positioning, Navigation, and Timing
792 Services. (The White House, Washington, DC), February 12, 2020.
793 <https://www.govinfo.gov/app/details/FR-2020-02-18/2020-03337>
- 794 [FCC] Federal Communications Commission (2020) Jammer Enforcement.
795 (FCC, Washington DC). Available at
796 <https://www.fcc.gov/general/jammer-enforcement>
- 797 [FCC E911] Federal Communications Commission (2020) Wireless E911 Location
798 Accuracy Requirements Sixth Report and Order and Order on
799 Reconsideration-PS Docket No. 07-114 (FCC, Washington DC).
800 Available at [https://docs.fcc.gov/public/attachments/DOC-](https://docs.fcc.gov/public/attachments/DOC-365168A1.pdf)
801 [365168A1.pdf](https://docs.fcc.gov/public/attachments/DOC-365168A1.pdf)
- 802 [FINRA 4590] Financial Industry Regulatory Authority (2016) *4590. Synchronization*
803 *of Member Business Clocks*. (FINRA, Washington, DC). Available at
804 <https://www.finra.org/rules-guidance/rulebooks/finra-rules/4590>
- 805 [GAL ICD] European GNSS (Galileo) Open Service (2021) *Signal-in-Space*
806 *Interface Control Document Issue 2.0*. (European Union). Available at
807 <https://www.gsc->

- 808 europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.0.pdf
809 [f](https://europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.0.pdf)
- 810 [GPS] Department of Homeland Security, US Coast Guard (1996) *Navstar*
811 *GPS User Equipment Introduction*. (U.S. Coast Guard Navigation
812 Center, Department of Homeland Security, Alexandria, VA), September
813 1996.
- 814 [GPS ICD-240] SAIC (GPS SE&I) (2021) *Navstar GPS Control Segment to User*
815 *Support Community*. (Air Force Space Command, Department of
816 Homeland Security, and the U.S. Coast Guard, Washington, DC),
817 Global Positioning System Interface Control Document ICD-GPS-
818 240C. Available [https://www.gps.gov/technical/icwg/ICD-GPS-](https://www.gps.gov/technical/icwg/ICD-GPS-240D.pdf)
819 [240D.pdf](https://www.gps.gov/technical/icwg/ICD-GPS-240D.pdf)
- 820 [GPS ICD-870] SAIC (GPS SE&I) (2020) *NAVSTAR Next Generation GPS Control*
821 *Segment (OCX) to User Support Community Interface*. (Air Force Space
822 Command, Department of Homeland Security, Department of
823 Transportation, Federal Aviation Administration, and the U.S. Coast
824 Guard, Washington, DC), Global Positioning System Interface Control
825 Document ICD-GPS-870E. Available at
826 <https://www.gps.gov/technical/icwg/ICD-GPS-870E.pdf>
- 827 [GPS GNSS] National Coordination Office for Space-Based Positioning, Navigation,
828 and Timing (2020) *Other Global Navigation Satellite Systems (GNSS)*.
829 Available at <https://www.gps.gov/systems/gnss/>
- 830 [GPS IS-200] SAIC (GPS SE&I) (2021) *NAVSTAR GPS Space Segment/Navigation*
831 *User Segment Interfaces*. (Air Force Space Command, Washington,
832 DC), Global Positioning System Interface Specification Document IS-
833 GPS- 200M. Available at [https://www.gps.gov/technical/icwg/IS-GPS-](https://www.gps.gov/technical/icwg/IS-GPS-200M.pdf)
834 [200M.pdf](https://www.gps.gov/technical/icwg/IS-GPS-200M.pdf)
- 835 [GPS IS-705] SAIC (GPS SE&I) (2021) *NAVSTAR GPS Space Segment/User Segment*
836 *L5 Interfaces*. (Air Force Space Command, Washington, DC), Global
837 Positioning System Interface Specification Document IS-GPS-705D.
838 Available at <https://www.gps.gov/technical/icwg/IS-GPS-705H.pdf>
- 839 [GPS IS-800] SAIC (GPS SE&I) (2021) *NAVSTAR GPS Space Segment/User Segment*
840 *L1C Interfaces*. (Air Force Space Command, Washington, DC), Global
841 Positioning System Interface Specification Document IS-GPS-800D.
842 Available at <https://www.gps.gov/technical/icwg/IS-GPS-800H.pdf>
- 843 [GPS SPS] U.S. Department of Defense (2020) *Global Positioning System (GPS)*
844 *Standard Positioning Service Performance Standard*, 5th Edition.
845 (Department of Defense, Washington, DC). Available at
846 <https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf>

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

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

854 [IEC 61850-90-4] International Electrotechnical Commission (2020) *IEC 61850-90-4:*
855 *2020 Communication Networks and Systems for Power Utility*
856 *Automation - Part 90-4: Network Engineering Guidelines* (IEC,
857 Geneva, Switzerland). Available at
858 <https://webstore.iec.ch/publication/64801>

859 [IEC 61850-90-12] International Electrotechnical Commission (2020) *IEC 61850-90-*
860 *12:2020 Communication networks and systems for power utility*
861 *automation - Part 90-12: Wide area network engineering guidelines*.
862 (IEC Geneva, Switzerland). Available at
863 <https://webstore.iec.ch/publication/63706>

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

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

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

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

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

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

- 886 *Generators* (IEEE SA, Piscataway, NJ). Available at doi:
887 10.1109/IEEESTD.2004.94440. (*Undergoing Revision*)
- 888 [IEEE 2030.101] IEEE Standards Association (2018) *IEEE 2030.101:2018 Guide for*
889 *Designing a Time Synchronization System for Power Substations* (IEEE
890 SA, Piscataway, NJ). Available at
891 https://standards.ieee.org/standard/2030_101-2018.html
- 892 [IETF 4082] Perrig A, Song D, Canetti D, Tygar, JD, Briscoe, B (2005) Timed
893 Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast
894 Source Authentication Transform Introduction (Internet Engineering
895 Task Force (IETF) Network Working Group), IETF Request for
896 Comments (RFC) 4082. Available at <https://tools.ietf.org/html/rfc4082>
- 897 [IETF 5905] Mills, D, Martin, J, Burbank, J, and Kach, W. ,*Network Time Protocol*
898 *Version 4: Protocol and Algorithms Specification*. (Internet Engineering
899 Task Force (IETF) Network Working Group) Available at
900 <https://datatracker.ietf.org/doc/html/rfc5905>
- 901 [IETF 7384] Mizrahi T (2014) Security Requirements for Time Protocols in Packet
902 Switched Networks. Introduction (Internet Engineering Task Force
903 (IETF) Network Working Group), IETF Request for Comments (RFC)
904 7384. Available at <https://tools.ietf.org/html/rfc7384>
- 905 [IETF 8573] Malhotra A, Goldberg S (2019) Message Authentication Code for the
906 Network Time Protocol (Internet Engineering Task Force (IETF)
907 Network Working Group), IETF Request for Comments (RFC) 8573.
908 Available at <https://tools.ietf.org/html/rfc8573>
- 909 [IETF 8633] Reilly D, Stenn H, Sibold D (2019) Network Time Protocol Best
910 Current Practices. (Internet Engineering Task Force (IETF) Network
911 Working Group), IETF Request for Comments (RFC) 8633. Available
912 at <https://tools.ietf.org/html/rfc8633>
- 913 [IETF 8915] Franke D, Sibold D, Danserie M, Sunblad R, Teichel K (2020) Using
914 the Network Time Security Specification to Secure the Network Time
915 Protocol. (Internet Engineering Task Force (IETF) Network Working
916 Group), IETF Request for Comments (RFC) 88915. Available at
917 <https://tools.ietf.org/html/rfc8915>
- 918 [IETF CMP] Haberman B (2020) Control Messages Protocol for Use with Network
919 Time Protocol. Internet Engineering Task Force (IETF) Network
920 Working Group), V4 Draft. Available at [https://tools.ietf.org/html/draft-](https://tools.ietf.org/html/draft-ietf-ntp-mode-6-cmds-10)
921 [ietf-ntp-mode-6-cmds-10](https://tools.ietf.org/html/draft-ietf-ntp-mode-6-cmds-10)
- 922 [IETF NTS] Franke D, Sibold D, Teichel K, Dansarie M, Sundblad R (2020)
923 Network Time Security for the Network Time Protocol Internet
924 Engineering Task Force (IETF) Network Time Protocol Working

- 925 Group). Available at [https://tools.ietf.org/html/draft-ietf-ntp-using-nts-](https://tools.ietf.org/html/draft-ietf-ntp-using-nts-for-ntp-28)
926 [for-ntp-28](https://tools.ietf.org/html/draft-ietf-ntp-using-nts-for-ntp-28)
- 927 [IMO 1575] International Maritime Organization (2017) MSC.1/Circular.1575 -
928 Guidelines for Shipborne Position, Navigation and Timing (PNT) Data
929 Processing Guidelines for Shipborne Position, Navigation and Timing.
930 (IMO, London, England). Available at
931 https://www.imorules.com/MSCCIRC_1575.html
- 932 [ISO 17025] International Organization for Standardization (2017) *ISO/IEC 17025*
933 *General Requirements for the Competence of Testing and Calibration*
934 *Laboratories*. (ISO, Geneva, Switzerland), Corrigendum 1, Mar. 2018.
935 Available at <https://www.iso.org/standard/66912.html>
- 936 [ITU-T 810] International Telecommunications Union Telecommunications
937 Standardization Sector (1996) *ITU-T G.810, Definitions and*
938 *Terminology for Synchronization Networks*. (ITU-T, Geneva,
939 Switzerland), Corrigendum 1, Nov. 2001. Available at
940 <https://www.itu.int/rec/T-REC-G.810/en>
- 941 [ITU- T G.8261] International Telecommunications Union Telecommunications
942 Standardization Sector (2019) *ITU-T G.8261/Y.1361 Timing and*
943 *synchronization aspects in packet networks*. (ITU-T, Geneva,
944 Switzerland). Available at [https://www.itu.int/rec/T-REC-G.8261-](https://www.itu.int/rec/T-REC-G.8261-201908-I/en)
945 [201908-I/en](https://www.itu.int/rec/T-REC-G.8261-201908-I/en)
- 946 [ITU- T G.8262] International Telecommunications Union Telecommunications
947 Standardization Sector (2018) *ITU-T G.8262/Y.1367 Timing*
948 *Characteristics of Primary Reference Time Clocks*. (ITU-T, Geneva,
949 Switzerland). Available at <https://www.itu.int/rec/T-REC-G.8262>
- 950 [ITU- T G.8272] International Telecommunications Union Telecommunications
951 Standardization Sector (2018) *ITU-T G.8262/Y.1367 Timing*
952 *Characteristics of Primary Reference Time Clocks*. (ITU-T, Geneva,
953 Switzerland). Available at <https://www.itu.int/rec/T-REC-G.8272/en>
- 954 [ITU-T G.8275.1] International Telecommunications Union Telecommunications
955 Standardization Sector (2022) *ITU-T G.8275.1/Y.1369.1 Amendment 3*
956 *Precision Time Protocol Telecom Profile for Phase/Time*
957 *Synchronization with Full Timing Support from The Network*. (ITU-T,
958 Geneva, Switzerland). Available at [https://www.itu.int/rec/T-REC-](https://www.itu.int/rec/T-REC-G.8275.1/en)
959 [G.8275.1/en](https://www.itu.int/rec/T-REC-G.8275.1/en)
- 960 [ITU-T GNSS] International Telecommunications Union Telecommunications
961 Standardization Sector (2020) *ITU-T GSTR-GNSS Considerations on*
962 *the use of GNSS as a primary time reference in telecommunications*
963 (ITU-T, Geneva, Switzerland). Available at
964 https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-HOME-2020-PDF-

965 [E.pdf](#)

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

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

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

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

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

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

989 [NDAA] Department of Defense, General Services Administration, and National
990 Aeronautics and Space Administration (2019) Interim Rule Issued by
991 DoD, GSA, and NASA (DoD, GSA, and NASA, Washington, DC).
992 Available at [https://www.acquisition.gov/FAR-Case-2019-](https://www.acquisition.gov/FAR-Case-2019-009/889_Part_B)
993 [009/889_Part_B](https://www.acquisition.gov/FAR-Case-2019-009/889_Part_B)

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

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

1000 [NERC GRIDEX] North American Electric Reliability Corporation (2020) *GridEx*.
1001 Available at <https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx>

1002 [NIST CSF] National Institute of Standards and Technology (2018) Framework for
1003 Improving Critical Infrastructure Cybersecurity, Version 1.1. (National
1004 Institute of Standards and Technology, Gaithersburg, MD).
1005 <https://doi.org/10.6028/NIST.CSWP.04162018>

1006 [NISTIR 8014] Hastings N, Franklin, J (2015) Considerations for Identity Management
1007 in Public Safety Mobile Networks. (National Institute of Standards and
1008 Technology, Gaithersburg, MD), NIST Interagency or Internal Report
1009 (IR) 8014. <https://doi.org/10.6028/NIST.IR.8014>

1010 [NISTIR 8320] Bartock M, Souppaya M, Savino R, Knoll T, Shetty U, Cherfaoui M,
1011 Yeluri R, Malhotra, Banks D, Jordan M, Pendarakis D, Rao, JR,
1012 Romness P, Scarfone K (2022) Hardware-Enabled Security: Enabling a
1013 Layered Approach to Platform Security for Cloud and Edge Computing
1014 Use Cases. (National Institute of Standards and Technology,
1015 Gaithersburg, MD).
1016 <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8320.pdf>

1017 [NIST JRES 120.017] Yao J, Levine J, Weiss M (2015) Toward Continuous GPS Carrier-Phase
1018 Time Transfer: Eliminating the Time Discontinuity at an Anomaly. NIST
1019 Journal of Research 120: 280-292. <https://doi.org/10.6028/jres.120.017>

1020 [NIST SP 250-29] Kamas G, Lombardi, M (2004) Remote Frequency Calibrations: The
1021 NIST Frequency Measurement and Analysis Service. (National Institute
1022 of Standards and Technology, Gaithersburg, MD), NIST Special
1023 Publication (SP) 250-29, Rev. E.
1024 [https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication250-
1025 29e2004.pdf](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication250-29e2004.pdf)

1026 [NIST SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting
1027 Risk Assessments. (National Institute of Standards and Technology,
1028 Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
1029 <https://doi.org/10.6028/NIST.SP.800-30r1>

1030 [NIST SP 800-34] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010)
1031 Contingency Planning Guide for Federal Information Systems.
1032 (National Institute of Standards and Technology, Gaithersburg, MD),
1033 NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of
1034 November 11, 2010. <https://doi.org/10.6028/NIST.SP.800-34r1>

1035 [NIST SP 800-37] Joint Task Force (2018) Risk Management Framework for Information
1036 Systems and Organizations: A System Life Cycle Approach for Security
1037 and Privacy. (National Institute of Standards and Technology,
1038 Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2.
1039 <https://doi.org/10.6028/NIST.SP.800-37r2>

1040 [NIST SP 800-39] Joint Task Force Transformation Initiative (2011) Managing
1041 Information Security Risk: Organization, Mission, and Information

- 1042 System View. (National Institute of Standards and Technology,
1043 Gaithersburg, MD), NIST Special Publication (SP) 800-39.
1044 <https://doi.org/10.6028/NIST.SP.800-39>
- 1045 [NIST SP 800-53] Joint Task Force Transformation Initiative (2020) Security and Privacy
1046 Controls for Federal Information Systems and Organizations. (National
1047 nstitute of Standards and Technology, Gaithersburg, MD), NIST Special
1048 Publication (SP) 800-53, Rev. 5, Includes updates as of December 10,
1049 2020. <https://doi.org/10.6028/NIST.SP.800-53r5>
- 1050 [NIST SP 800-61] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer
1051 Security Incident Handling Guide. (National Institute of Standards and
1052 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61,
1053 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-61r2>
- 1054 [NIST SP 800-1115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical
1055 Guide to Information Security Testing and Assessment. (National
1056 Institute of Standards and Technology, Gaithersburg, MD), NIST
1057 Special Publication (SP) 800-115. <https://doi.org/10.6028/NIST.SP.800-115>
1058
- 1059 [NIST SP 800-160] Ross, R, Graubart, R, Bodeau, D, McQuaid, R (2016) Systems Security
1060 Engineering: Cyber Resiliency Considerations for the Engineering of
1061 Trustworthy Secure Systems (National Institute of Standards and
1062 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-
1063 160, Vol. 1, Rev.1. <https://doi.org/10.6028/NIST.SP.800-160v1>
- 1064 [NIST SP 800-160-2] Ross, R, Pillitteri VY, Graubart, R, Bodeau, D, McQuaid, R (2021)
1065 Systems Security Engineering: Cyber Resiliency Considerations for the
1066 Engineering of Trustworthy Secure Systems (National Institute of
1067 Standards and Technology, Gaithersburg, MD), NIST Special
1068 Publication (SP) 800-160, Vol. 2, Rev. 1.
1069 <https://doi.org/10.6028/NIST.SP.800-160v2r1>
- 1070 [NIST SP 800-161] Boyens J, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Supply
1071 Chain Risk Management Practices for Federal Information Systems and
1072 Organizations, (National Institute of Standards and Technology,
1073 Gaithersburg, MD), NIST Special Publication (SP) 800-161, Rev. 1.
1074 Available at
1075 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf>
1076
- 1077 [NIST SP 800-184] Bartock MJ, Scarfone KA, Smith MC, Witte GA, Cichonski JA,
1078 Souppaya MP (2016) Guide for Cybersecurity Event Recovery.
1079 (National Institute of Standards and Technology, Gaithersburg, MD),
1080 NIST Special Publication (SP) 800-184.
1081 <https://doi.org/10.6028/NIST.SP.800-184>

- 1082 [NIST SP 1065] Riley W, Howe DA (2008) Handbook of Frequency Stability Analysis.
1083 (National Institute of Standards and Technology, Gaithersburg, MD),
1084 NIST Special Publication (SP) 1065. Available at
1085 https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50505
- 1086 [NIST T&F Glossary] NIST Physical Measurement Laboratory, Time and Frequency Division
1087 (2020) *Time and Frequency Glossary from A to Z*. Available at
1088 [https://www.nist.gov/pml/time-and-frequency-division/popular-](https://www.nist.gov/pml/time-and-frequency-division/popular-links/time-frequency-z)
1089 [links/time- frequency-z](https://www.nist.gov/pml/time-and-frequency-division/popular-links/time-frequency-z)
- 1090 [NIST TN 1366] Volk, CM, Levine, J (1994) Analytical Estimation of Carrier Multipath
1091 Bias on GPS Position Measurements. (National Institute of Standards
1092 and Technology, Gaithersburg, MD), NIST Technical Note (TN) 1366.
1093 Available at <http://doi.org/10.6028/NIST.TN.1366>
- 1094 [NIST TN 2187] Sherman JA, Arissian L, Brown RC, Deutch MJ, Donley EA, Gerginov
1095 V, Levine J, Nelson GK, Novick AN, Patla BR, Parker TE, Stuhl BK,
1096 Sutton DD, Yao J, Yates WC, Zhang V and Lombardi MA (2021) A
1097 Resilient Architecture for the Realization and Distribution of
1098 Coordinated Universal Time to Critical Infrastructure Systems in the
1099 United States. (National Institute of Standards and Technology,
1100 Gaithersburg, MD), NIST Technical Note (TN) 2187. Available at
1101 <https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2187.pdf>
- 1102 [NIST USNO] NIST Physical Measurement Laboratory, Time and Frequency Division
1103 (2022) NIST USNO. Available at [https://www.nist.gov/pml/time-and-](https://www.nist.gov/pml/time-and-frequency-division/time-services/nist-usno)
1104 [frequency-division/time-services/nist-usno](https://www.nist.gov/pml/time-and-frequency-division/time-services/nist-usno)
- 1105 [NOAA SWS] NOAA Space Weather Prediction Center (2022) NOAA Space Weather
1106 Scales. Available at [https://www.swpc.noaa.gov/noaa-scales-](https://www.swpc.noaa.gov/noaa-scales-explanation)
1107 [explanation](https://www.swpc.noaa.gov/noaa-scales-explanation)
- 1108 [NTP MON] Network Time Protocol (2020) *Who is using my NTP server?* Available at
1109 <http://support.ntp.org/bin/view/Support/MonitoringAndControllingNTP#>
1110 [Who_is_using_my_NTP_server](http://support.ntp.org/bin/view/Support/MonitoringAndControllingNTP#Who_is_using_my_NTP_server)
- 1111 [NTP SEC] Network Time Protocol (2020) *NTP Security Notice*. Available at
1112 <http://support.ntp.org/bin/view/Main/SecurityNotice>
- 1113 [PPD-21] Presidential Policy Directive (PPD)-21 (2013) Critical Infrastructure
1114 Security and Resilience. (The White House, Washington, DC),
1115 DCPD201300092, February 12, 2013.
1116 [https://www.govinfo.gov/content/pkg/DCPD-201300092/html/DCPD-](https://www.govinfo.gov/content/pkg/DCPD-201300092/html/DCPD-201300092.htm)
1117 [201300092.htm](https://www.govinfo.gov/content/pkg/DCPD-201300092/html/DCPD-201300092.htm)
- 1118 [RTCA 229] Radio Technical Commission for Aeronautics (2020) *RTCA DO-229*
1119 *Minimum Operational Performance Standards for Global Positioning*

1120 *Systems/Satellite-Based Augmentation System Airborne Equipment.*
1121 (RTCA, Washington, DC). Available at
1122 https://my.rtca.org/NC_Product?id=a1B36000001IckIEAC

1123 [RTCA 235] Radio Technical Commission for Aeronautics (2008) *RTCA DO-235A*
1124 *Assessment of Radio Frequency Interference Relevant to the GNSS L1*
1125 *Frequency Band.* (RTCA, Washington, DC). Available at
1126 https://my.rtca.org/NC_Product?id=a1B36000001IckKEAS

1127 [RTCA 292] Radio Technical Commission for Aeronautics (2004) *RTCA DO-292*
1128 *Assessment of Radio Frequency Interference Relevant to the GNSS*
1129 *L5/E5A Frequency Band.* (RTCA, Washington, DC). Available at
1130 https://my.rtca.org/nc_store?search=292

1131 [RTCA 316] Radio Technical Commission for Aeronautics (2009) *RTCA DO-316*
1132 *Minimum Operational Performance Standards for Global Positioning*
1133 *System/Aircraft Base Augmentation System.* (RTCA, Washington, DC).
1134 Available at https://my.rtca.org/nc_store?search=316

1135 [RTCA 326] Radio Technical Commission for Aeronautics (2010) *RTCA D DO-326 -*
1136 *Airworthiness Security Process Specification.* (RTCA, Washington,
1137 DC). Available at https://my.rtca.org/nc_store?search=326

1138 [RTCA 356] Radio Technical Commission for Aeronautics (2018) *RTCA DO-356A*
1139 *Airworthiness Security Methods and Considerations.* (RTCA,
1140 Washington, DC). Available at [https://my.rtca.org/NC](https://my.rtca.org/NC_Product?id=a1B36000001IckEAC)
1141 [Product?id=a1B36000001IckEAC](https://my.rtca.org/NC_Product?id=a1B36000001IckEAC)

1142 [SEC 613] Securities Exchange Commission (2020) Rule 613 (Consolidated Audit
1143 Trail.) (SEC, Washington, DC). Available at
1144 <https://www.sec.gov/divisions/marketreg/rule613-info.htm>

1145 [SNMP3] Case J et. al. Simple Network Management Protocol, Version 3 (Internet
1146 Engineering Task Force (IETF) Network Working Group), IETF
1147 Request for Comments (RFC) 3410 through (RFC) 3418. Available at
1148 <https://tools.ietf.org/html/rfc3410>, <https://tools.ietf.org/html/rfc3411>,
1149 <https://tools.ietf.org/html/rfc3412>,
1150 <https://tools.ietf.org/html/rfc3413>, <https://tools.ietf.org/html/rfc3414>,
1151 <https://tools.ietf.org/html/rfc3415>, <https://tools.ietf.org/html/rfc3416>,
1152 <https://tools.ietf.org/html/rfc3417>, <https://tools.ietf.org/html/rfc3418>

1153 [SNMPSEC] Cybersecurity & Infrastructure Security Agency (2017) Reducing the
1154 Risk of SNMP Abuse. Alert (TA17-156A) (DHS, Washington, DC).
1155 Available at <https://us-cert.cisa.gov/ncas/alerts/TA17-156A>

1156 [SPD-7] Space Policy Directive 7 (SPD)-7 (2021) The United States Space-
1157 Based Positioning, Navigation, and Timing Policy. (The White House,
1158 Washington, DC), DCPD-202100025, January 15, 2021. Available at

- 1159 <https://www.govinfo.gov/app/details/DCPD-202100025>
1160 [USG FRP] Department of Defense, Department of Homeland Security, and
1161 Department of Transportation (2021) 2021 Federal Radionavigation
1162 Plan (Department of Transportation, Washington DC). Available at
1163 <https://www.transportation.gov/pnt/radionavigation-systems-planning>
- 1164 [USNG] Federal Geographic Data Committee (2001) Standard for A U.S.
1165 National Grid, FGDC-STD-011-2001. (FGDC, Reston, VA). Available
1166 at
1167 https://www.fgdc.gov/standards/projects/usng/TFIGURES_6.pdf/at_download/file
1168
- 1169 [USNO GPS] United States Naval Observatory (2022) GPS Time Transfer (US Navy,
1170 Washington DC). Available at
1171 <https://www.cnmoc.usff.navy.mil/Organization/United-States-Naval-Observatory/Precise-Time-Department/Global-Positioning-System/USNO-GPS-Time-Transfer/>
1172
1173

1174 **Appendix A— Acronyms and Abbreviations**

1175 Selected acronyms and abbreviations used in this document are defined below.

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

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

1176 **Appendix B— Glossary**

1177 Selected terms used in this document are defined below.

1178 **Accuracy (Absolute):** The degree of conformity of a measured or calculated value to
1179 the true value, typically based on a global reference system. For time, the global
1180 reference can be based on the following time scales: UTC, TAI, or GPS. For position,
1181 the global reference can be WGS-84.

1182 **Accuracy (Relative):** The degree of agreement between measured or calculated values
1183 among the devices and applications dependent on the position, navigation, or time data
1184 at an instant in time.

1185 **Agility:** The property of a system or an infrastructure that can be reconfigured, in which
1186 resources can be reallocated, and in which components can be reused or repurposed so
1187 that cyber defenders can define, select, and tailor cyber courses of action for a broad
1188 range of disruptions or malicious cyber activities. [NIST SP 800-160]

1189 **Allan deviation:** A non-classical statistic used to estimate stability. The NIST
1190 equation for the Allan deviation (with non-overlapping samples) is

1191
$$\sigma_y(\tau) = \sqrt{\frac{1}{2(M-1)} \sum_{i=1}^{M-1} (\bar{y}_{i+1} - \bar{y}_i)^2}$$

1192 where \bar{y}_i is the i^{th} of M frequency offset averages over the observation period, τ . Or

1193
$$\sigma_y(\tau) = \sqrt{\frac{1}{2\tau^2(N-2)} \sum_{i=1}^{N-2} (x_{i+2} - 2x_{i+1} + x_i)^2}$$

1194 where x_i is a series of phase offset measurements in time units that consists of individual
1195 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
1196 equally spaced in intervals τ seconds long.

1197 The confidence interval of an Allan deviation estimate is dependent on the noise type but is often
1198 estimated as $\frac{\sigma_y(\tau)}{\sqrt{N}}$. [NIST T&F Glossary, Adapted] [NIST SP 1065, Adapted]

1199 **Atomic Clock:** A clock referenced to an atomic oscillator. Only clocks with an internal atomic
1200 oscillator qualify as atomic clocks. [NIST T&F Glossary, Adapted]

1201 **Atomic Oscillator:** An oscillator that uses the quantized energy levels in atoms or molecules as
1202 the source of its resonance. The laws of quantum mechanics dictate that the energies of a bound
1203 system, such as an atom, have certain discrete values. An electromagnetic field at a particular
1204 frequency can boost an atom from one energy level to a higher one, or an atom at a high energy
1205 level can drop to a lower level by emitting energy. The resonance frequency, f_0 , of an atomic
1206 oscillator is the difference between the two energy levels divided by Planck's constant, h .

1207 The principle underlying the atomic oscillator is that since all atoms of a specific element are

1208 identical, they should produce exactly the same frequency when they absorb or release energy. In
1209 theory, the atom is a perfect “pendulum” whose oscillations are counted to measure a time
1210 interval. The national frequency standards developed by NIST and other laboratories derive their
1211 resonance frequency from the cesium atom and typically use cesium fountain technology.
1212 Rubidium oscillators are the lowest priced and most common atomic oscillators, but cesium
1213 beam and hydrogen maser atomic oscillators are also sold commercially in much smaller
1214 quantities. [NIST T&F Glossary]

1215 **Attack:** Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy
1216 information system resources or the information itself. [CNSSI 4009]

1217 **Availability (PNT):** The availability of a PNT system is the percentage of time that the services
1218 of the system are usable. Availability is an indication of the ability of the system to provide
1219 usable service within the specified coverage area. Signal availability is the percentage of time
1220 that PNT signals transmitted from external sources are available for use. Availability is a
1221 function of both the physical characteristics of the environment and the technical capabilities of
1222 the PNT service provider. [USG FRP Appendix E, Adapted]

1223 **Calibration:** A comparison between a device under test and an established standard, such as
1224 UTC(NIST). When the calibration is finished, it should be possible to state the estimated time
1225 offset and/or frequency offset of the device under test with respect to the standard, as well as the
1226 measurement uncertainty. Calibrations can be absolute or relative. Absolute calibrations are not
1227 biased by the calibration reference and would, therefore, be more reproducible. However,
1228 absolute calibrations can be more complex to determine. The bias in relative calibrations would
1229 be consistent if all the devices in the system are calibrated against the same calibration reference.
1230 Calibrations may also be performed relative to other devices without reference to an absolute
1231 standard. Relative calibrations are generally simpler to perform than absolute calibrations. [NIST
1232 T&F Glossary, Adapted]

1233 **Characterization:** An extended test of the performance characteristics of a clock or oscillator. A
1234 characterization involves more work than a typical calibration. The device under test is usually
1235 measured for a long period of time (days or weeks), and sometimes, a series of measurements is
1236 made under different environmental conditions. A characterization is often used to determine the
1237 types of noise that limit the uncertainty of the measurement and the sensitivity of the device to
1238 environmental changes. [NIST T&F Glossary]

1239 **Clock:** A device that generates periodic, accurately spaced signals for timekeeping applications.
1240 A clock consists of at least three parts: an oscillator, a device that counts the oscillations and
1241 converts them to units of time interval (such as seconds, minutes, hours, and days), and a means
1242 of displaying or recording the results. [NIST T&F Glossary]

1243 **Component:** A hardware, software, firmware part or element of a larger PNT system with well-
1244 defined inputs and outputs and a specific function. [NIST SP 800-160, Adapted][DHS RCF,
1245 Adapted]

1246 **Confidentiality:** Preserving authorized restrictions on information access and disclosure,
1247 including means for protecting personal privacy and proprietary information. [NIST FIPS 200]

- 1248 **Continuity:** The probability that the specified PNT system performance will be maintained for
1249 the duration of a phase of operation, presuming that the PNT system was available at the
1250 beginning of that phase of operation. [USG FRP]
- 1251 **Coverage:** The surface area or space volume in which the signals are adequate to permit the user
1252 to determine a position to a specified level of accuracy. Coverage is influenced by system
1253 geometry, signal power levels, receiver sensitivity, atmospheric noise conditions, and other
1254 factors that affect signal availability. [USG FRP]
- 1255 **Cybersecurity:** Prevention of damage to, protection of, and restoration of computers, electronic
1256 communications systems, electronic communications services, wire communication, and
1257 electronic communication, including information contained therein, to ensure its availability,
1258 integrity, authentication, confidentiality, and nonrepudiation. For example, PNT data is
1259 generated by cyber systems. Protection of the devices and systems used to generate PNT data
1260 should be considered part of cybersecurity. [NIST SP 800-53]
- 1261 **Delay (Path Delay):** The [signal] delay between a transmitter and a receiver. Path delay is often
1262 the largest contributor to time transfer uncertainty. For example, consider a radio signal
1263 broadcast over a 1000 km path. Since radio signals travel at the speed of light (with a delay of
1264 about 3.3 $\mu\text{s}/\text{km}$), we can calibrate the 1000 km path by estimating the path delay as 3.3 ms and
1265 applying a 3.3 ms correction to our measurement. Sophisticated time transfer systems, such as
1266 GPS, automatically correct for path delay. The absolute path delay is not important to frequency
1267 transfer systems because on-time pulses are not required, but variations in path delay still limit
1268 the frequency uncertainty. [NIST T&F Glossary, Adapted]
- 1269 **Disciplined Oscillator (DO):** An oscillator whose output frequency is continuously adjusted
1270 (often through the use of a phase locked loop) to agree with an external reference. For example, a
1271 GPS disciplined oscillator (GPSDO) usually consists of a quartz or rubidium oscillator whose
1272 output frequency is continuously adjusted to agree with signals broadcast by the GPS satellites.
- 1273 **Frequency:** The rate of a repetitive event. If T is the period of a repetitive event, then the
1274 frequency f is its reciprocal, $1/T$. Conversely, the period is the reciprocal of the frequency, $T = 1$
1275 $/f$. Because the period is a time interval expressed in seconds (s), it is easy to see the close
1276 relationship between time interval and frequency. The standard unit for frequency is the hertz
1277 (Hz), defined as the number of events or cycles per second. The frequency of electrical signals is
1278 often measured in multiples of hertz, including kilohertz (kHz), megahertz (MHz), or gigahertz
1279 (GHz). [NIST T&F Glossary]
- 1280 **Frequency Accuracy:** The degree of conformity of a measured or calculated frequency to its
1281 definition. Because accuracy is related to the offset from an ideal value, frequency accuracy is
1282 usually stated in terms of the frequency offset. [NIST T&F Glossary]
- 1283 **Frequency Drift:** An undesired progressive change in frequency with time. Frequency drift can
1284 be caused by instability in the oscillator and environmental changes, although it is often hard to
1285 distinguish between drift and oscillator aging. Frequency drift may be in either direction
1286 (resulting in a higher or lower frequency) and is not necessarily linear. [NIST T&F Glossary]
- 1287 **Frequency Offset:** The difference between a measured frequency and an ideal frequency with

1288 zero uncertainty. This ideal frequency is called the nominal frequency. [NIST T&F Glossary]

1289 Frequency offset can be measured in either the frequency domain or the time domain. A simple
1290 frequency domain measurement involves directly counting and displaying the output frequency of
1291 the device under test with a frequency counter. The frequency offset is calculated as

1292
$$f_{off} = \frac{f_{meas} - f_{nom}}{f_{nom}}$$

1293 where f_{meas} is the reading from the frequency counter, and f_{nom} is the specified output frequency of
1294 the device under test.

1295 Frequency offset measurements in the time domain involve measuring the time difference
1296 between the device under test and the reference. The time interval measurements can be made
1297 with an oscilloscope or a time interval counter. If at least two time interval measurements are
1298 made, frequency offset can be estimated as

1299
$$f_{off} = -\frac{\Delta t}{T}$$

1300 where Δt is the difference between time interval measurements (phase difference), and T is the
1301 measurement period. [NIST T&F Glossary, Adapted]

1302 **Frequency Stability:** The degree to which an oscillating signal produces the same frequency for
1303 a specified interval of time. It is important to note the time interval—some devices have good
1304 short-term stability while others have good long-term stability. Stability does not determine
1305 whether the frequency of a signal is right or wrong. It only indicates whether that frequency stays
1306 the same. The Allan deviation is the most common metric used to estimate frequency stability,
1307 but several similar statistics are also used. [NIST T&F Glossary]

1308 **Global Navigation Satellite System (GNSS):** GNSS collectively refers to the worldwide
1309 positioning, navigation, and timing (PNT) determination capability available from one or more
1310 satellite constellations. Each GNSS system employs a constellation of satellites that operate in
1311 conjunction with a network of ground stations. Receivers and system integrity monitoring are
1312 augmented as necessary to support the required position, navigation, and timing performance for
1313 the intended operation. [USG FRP, Adapted] [ICAO 9849, Adapted]

1314 **GPS:** The Global Positioning System (GPS) is a U.S.-owned utility that provides users with
1315 positioning, navigation, and timing (PNT) services. This system consists of three segments: the
1316 space segment, the control segment, and the user segment. The U.S. Space Force develops,
1317 maintains, and operates the space and control segments. [GPS GNSS]

1318 **Holdover:** An operating condition of a clock which has lost its controlling reference input, is using
1319 its local oscillator, and can be augmented with stored data acquired while locked to the reference
1320 input or a frequency reference to control its output.

1321 **Integrity:** A measure of the trust that can be placed in the correctness of the information
1322 supplied by a PNT service provider. Integrity includes the ability of the system to provide timely

- 1323 warnings to users when the PNT data should not be used. [USG FRP]
- 1324 **Interchangeable:** The ability to combine signals from multiple PNT data sources into a single
1325 PNT solution, as well as the ability to provide a solution from an alternative source when a
1326 primary source is not available. [USG FRP]
- 1327 **Interference (electromagnetic):** Any electromagnetic disturbance that interrupts, obstructs,
1328 degrades, or otherwise limits the performance of user equipment. [USG FRP, Appendix E]
- 1329 **Jamming (electromagnetic):** The deliberate radiation, reradiation, or reflection of
1330 electromagnetic energy for the purpose of preventing or reducing the effective use of a signal.
1331 [USG FRP, Appendix E]
- 1332 **Jitter:** The short-term variations of the significant instants of a timing signal from their ideal
1333 positions in time (where short-term implies that these variations are of frequency greater than or
1334 equal to 10 Hz). [ITU-T 810]
- 1335 **Leap Second:** A second added to Coordinated Universal Time (UTC) to make it agree with
1336 astronomical time to within 0.9 second. UTC is an atomic time scale based on the performance
1337 of atomic clocks. Astronomical time is based on the rotational rate of the Earth. Since atomic
1338 clocks are more stable than the rate at which the Earth rotates, leap seconds are needed to keep
1339 the two time scales in agreement. [NIST T&F Glossary, Adapted]
- 1340 **Multipath:** The propagation phenomenon that results in signals reaching the receiving antenna
1341 by two or more paths. When two or more signals arrive simultaneously, wave interference
1342 results. The received signal fades if the wave interference is time varying or if one of the
1343 terminals is in motion. [USG FRP, Appendix E]
- 1344 **Navigation:** The ability to determine a current and desired position (relative or absolute) and
1345 apply corrections to course, orientation, and speed to attain a desired position. Navigation
1346 coverage requirements could be global, from sub-surface to surface and from surface to space.
1347 [DOT, Adapted]
- 1348 **Nominal Frequency:** An ideal frequency with zero uncertainty. The nominal frequency is the
1349 frequency labeled on an oscillator's output. For this reason, it is sometimes called the nameplate
1350 frequency. For example, an oscillator whose nameplate or label reads 5 MHz has a nominal
1351 frequency of 5 MHz. The difference between the nominal frequency and the actual output
1352 frequency of the oscillator is the frequency offset. [NIST T&F Glossary]
- 1353 **Oscillator:** An electronic device used to generate an oscillating signal. The oscillation is based
1354 on a periodic event that repeats at a constant rate. The device that controls this event is called a
1355 resonator. The resonator needs an energy source so it can sustain oscillation. Taken together, the
1356 energy source and resonator form an oscillator. Although many simple types of oscillators (both
1357 mechanical and electronic) exist, the two types of oscillators primarily used for time and
1358 frequency measurements are quartz oscillators and atomic oscillators. [NIST T&F Glossary]
- 1359 **PNT Data:** All information used to form or disseminate PNT solutions, including signals,
1360 waveforms, and network packets.

- 1361 **PNT Solution:** The full solution provided by a PNT system or source, including time, position,
1362 and velocity. A PNT system or source may provide a full PNT solution or a part of it. For
1363 example, a GNSS receiver provides a full PNT solution, while a local clock provides only a
1364 timing or frequency solution. [DHS RCF]
- 1365 **PNT Source:** A PNT system component that is used to produce a PNT solution. Examples
1366 include GNSS receivers, networked and local clocks, inertial navigation systems (INS), and
1367 timing services provided over a wired or wireless connection. [DHS RCF]
- 1368 **PNT System:** The components, processes, and parameters that collectively produce the final
1369 PNT solution for the consumer. [DHS RCF]
- 1370 **Phase:** The position of a point in time (instant) on a waveform cycle. A complete cycle is
1371 defined as the interval required for the waveform to retain its arbitrary initial value. [NIST T&F
1372 Glossary]
- 1373 **Phenomenologies:** Physical phenomena such as radio frequencies, inertial sensors, and scene
1374 mapping, as well as diverse sources and data paths using those physical phenomena (e.g.,
1375 multiple radio frequencies) to provide interchangeable solutions to users to ensure robust
1376 availability. [USG FRP]
- 1377 **Positioning:** The ability to accurately and precisely determine one's location and orientation
1378 two-dimensionally (or three-dimensionally, when required) referenced to a standard reference
1379 frame, such as the World Geodetic System 1984, WGS84[G873], or ITRF2014. [DOT]
- 1380 **Precision:** Refers to how closely individual PNT measurements agree with each other. [USG
1381 FRP]
- 1382 **Proper Working State:** A condition in which the device or system contains no compromised
1383 internal components or data fields (e.g., data stored to memory) and from which the device or
1384 system can recognize and process valid input signals and output valid PNT solutions. An initial
1385 pre-deployment configuration is a basic example. The accuracy of the immediate PNT solution is
1386 not specified in this definition, as it will depend on the specifics of the device or system's
1387 performance and the degradation allowed by different resilience levels. [DHS RCF]
- 1388 **Reliability:** The probability of performing a specified function without failure under given
1389 conditions for a specified period of time. [USG FRP]
- 1390 **Residual Risk:** Portion of risk remaining after security measures have been applied. [CNSSI
1391 4009]
- 1392 **Resilience:** The ability to prepare for and adapt to changing conditions and withstand and
1393 recover rapidly from disruptions. Resilience includes the ability to withstand and recover from
1394 deliberate attacks, accidents, or naturally occurring threats or incidents. [PPD-21]
- 1395 **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or
1396 event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or
1397 event occurs; and (ii) the likelihood of occurrence. [NIST SP 800-37]

1398 **Risk Assessment:** The process of identifying, estimating, and prioritizing risks to organizational
1399 operations (including mission, functions, image, reputation), organizational assets, individuals,
1400 other organizations, and the Nation, resulting from the operation of an information system. Part
1401 of risk management incorporates threat and vulnerability analyses, and considers mitigations
1402 provided by security controls planned or in place. Synonymous with risk analysis. [NIST SP
1403 800-30]

1404 **Risk Management:** The program and supporting processes to manage information security risk
1405 to organizational operations (including mission, functions, image, reputation), organizational
1406 assets, individuals, other organizations, and the Nation and includes (i) establishing the context
1407 for risk-related activities, (ii) assessing risk, (iii) responding to risk once determined, and (iv)
1408 monitoring risk over time. [NIST SP 800-39]

1409 **Risk Management Framework:** The Risk Management Framework (RMF), presented in NIST
1410 SP 800-37, provides a disciplined and structured process that integrates information security and
1411 risk management activities into the system development life cycle. [NIST SP 800-37]

1412 **Secure:** To reduce the risks of intrusions and attacks as well as the effects of natural or manmade
1413 disasters on critical infrastructure by physical means or defensive cyber measures. [PPD-21]

1414 **Short-Term Stability:** The stability of a time or frequency signal over a short measurement
1415 interval, usually an interval of 100 seconds or less in duration. [NIST T&F Glossary]

1416 **Stability:** An inherent characteristic of an oscillator that determines how well it can produce the
1417 same frequency over a given time interval. Stability does not indicate whether the frequency is
1418 right or wrong, but only whether it stays the same. The stability of an oscillator does not
1419 necessarily change when the frequency offset changes. An oscillator can be adjusted, and its
1420 frequency moved either further away from or closer to its nominal frequency without changing
1421 its stability at all.

1422 The stability of an oscillator is usually specified by a statistic, such as the Allan deviation, that
1423 estimates the frequency fluctuations of the device over a given time interval. Some devices, such
1424 as an OCXO [Oven Controlled Crystal (Xtal) Oscillator] have good short-term stability and poor
1425 long-term stability. Other devices, such as a GPS disciplined oscillator (GPSDO), typically have
1426 poor short-term stability and good long-term stability. [NIST T&F Glossary, Adapted]

1427 **Synchronization:** The process of setting two or more clocks to the same time. [NIST T&F
1428 Glossary]

1429 **Syntonization:** The process of setting two or more oscillators to the same frequency. [NIST
1430 T&F Glossary]

1431 **Threat:** Any circumstance or event with the potential to adversely impact organizational
1432 operations, organizational assets, individuals, other organizations, or the Nation through a system
1433 via unauthorized access, destruction, disclosure, modification of information, or denial of
1434 service. [NIST SP 800-53]

1435 **Traceability, Metrological:** Property of a measurement result whereby the result can be related

- 1436 to a reference through a documented, unbroken chain of calibrations, each contributing to the
1437 measurement uncertainty. [VIM]
- 1438 **Time Interval:** The elapsed time between two events. In time and frequency metrology, time
1439 interval is usually measured in small fractions of a second, such as milliseconds, microseconds,
1440 or nanoseconds. Higher resolution time interval measurements are often made with a time
1441 interval counter. [NIST T&F Glossary]
- 1442 **Time Scale:** An agreed upon system for keeping time. All time scales use a frequency source to
1443 define the length of the second, which is the standard unit of time interval. Seconds are then
1444 counted to measure longer units of time interval, such as minutes, hours, or days. Modern time
1445 scales, such as UTC, define the second based on an atomic property of the cesium atom, and thus
1446 standard seconds are produced by cesium oscillators. Earlier time scales (including earlier
1447 versions of Universal Time) were based on astronomical observations that measured the
1448 frequency of the Earth's rotation. [NIST T&F Glossary]
- 1449 **Validation:** Confirmation (through the provision of strong, sound, and objective evidence and
1450 demonstration) that requirements for a specific intended use or application have been fulfilled
1451 and that the system, while in use, fulfills its mission or business objectives while being able to
1452 provide adequate protection for stakeholder and mission or business assets, minimize or contain
1453 asset loss and associated consequences, and achieve its intended use in its intended operational
1454 environment with the desired level of trustworthiness. [NIST SP 800-160, §3.4.11, Adapted]
- 1455 **Verification:** Process of producing objective evidence that sufficiently demonstrates that the
1456 system satisfies its security requirements and security characteristics with the level of assurance
1457 that applies to the system. [NIST SP 800-160, §3.4.9, Adapted]
- 1458 **Vulnerability:** A weakness in an information system, system security procedures, internal
1459 controls, or implementation that could be exploited or triggered by a threat source. [NIST SP
1460 800-30]
- 1461 **Wander:** The long-term variations—random walk frequency noise—of the significant instants
1462 of a digital signal from their ideal position in time (where long-term implies that these variations
1463 are of frequency less than 10 Hz). [ITU-T 810, Adapted]
- 1464 **World Geodetic System 1984 (WGS 84):** An Earth-centered, Earth-fixed terrestrial reference
1465 system and geodetic datum. WGS 84 is based on a consistent set of constants and model
1466 parameters that describe the Earth's size, shape, gravity, and geomagnetic fields. WGS 84 is the
1467 standard U.S. Department of Defense definition of a global reference system for geospatial
1468 information and is the reference system for GPS. It is consistent with the International Terrestrial
1469 Reference System (ITRS). [USG FRP]

1470 **Appendix C—Additional Resources**

- 1471 3rd Generation Partnership Project (2020) *3GPP TS 22.104 Service Reequipments for Cyber-*
1472 *physical Control Applications in Vertical Domains*. (3GPP, Sophia Antipolis, France). Available
1473 at
1474 [https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3528)
1475 [=3528](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3528)
- 1476 3rd Generation Partnership Project (2018) *R2-1817172 Overview of UE Time Synchronization*
1477 *Methods*. (3GPP, Sophia Antipolis, France). Available at
1478 https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_104/Docs/R2-1817172.zip
- 1479 3rd Generation Partnership Project (2020) *SID: Feasibility Study on 5G Timing Resiliency System*
1480 *FS 5TRS*. (3GPP, Sophia Antipolis, France). Available at
1481 <https://portal.3gpp.org/ngppapp/CreateTDoc.aspx?mode=view&contributionUid=S1-202281>
- 1482 [https://www.afrl.af.mil/News/Article/2874807/afrls-pnt-agilepod-achieves-flight-test-](https://www.afrl.af.mil/News/Article/2874807/afrls-pnt-agilepod-achieves-flight-test-objectives/https://doi.org/10.21236/ADA290597)
1483 [objectives/https://doi.org/10.21236/ADA290597](https://www.afrl.af.mil/News/Article/2874807/afrls-pnt-agilepod-achieves-flight-test-objectives/https://doi.org/10.21236/ADA290597) or
1484 <https://afresearchlab.com/technology/sensors/agilepod/>
- 1485 ATIS (2017) *ATIS-0900005 GPS Vulnerability*. (ATIS, Washington, DC). Available at
1486 https://access.atis.org/apps/group_public/download.php/36304/ATIS-0900005.pdf
- 1487 Allan DW, Weiss MA (1980) Accurate Time and Frequency Transfer During Common-View of
1488 a GPS Satellite, *34th Annual Frequency Control Symposium*, (U.S. Army Electronic Research
1489 and Development Command, Philadelphia, PA) pp. 334-346. Available at
1490 <https://apps.dtic.mil/dtic/tr/fulltext/u2/a213670.pdf>
- 1491 Anand DM, Freiheit C, Weiss, MA, Shenoi K, Ossareh H (2019) A Timing Impairment Module
1492 for Electrical Synchro metrology. *2019 IEEE International Symposium on Precision Clock*
1493 *Synchronization for Measurement, Control, and Communication (ISPCS)*, (IEEE, Portland, OR),
1494 pp. 1-7. Available at <https://ieeexplore.ieee.org/document/8886638>
- 1495 Boehm BW (1991) Software risk management: Principles and practices. *IEEE Software*, vol. 8,
1496 no.1, pp. 32–41. Available at <https://doi.org/10.1109/52.62930>
- 1497 Communications Security, Reliability, And Interoperability Council VII (2020) Final Report -
1498 Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation. (*Working Group 2:*
1499 *Managing Security Risk in the Transition to 5, CSRIC, Washington, DC*). Available at
1500 <https://www.fcc.gov/file/18918/download>
- 1501 CTIA (2019) Protecting America’s Next-Generation Networks (CTIA, Washington, DC). Available
1502 at https://api.ctia.org/wp-content/uploads/2018/07/ProtectingAmericasNetworks_FINAL.pdf
- 1503 Department of Defense. (2015) *DoD Program Manager’s Guidebook for Integrating the Cybersecurity*
1504 *Risk Management Framework (RMF) into the System Acquisition Lifecycle*. (DOD, Washington, DC).
1505 Available at <https://www.dau.edu/tools/Lists/DAUTools/Attachments/37/DoD%20->

- 1506 [%20Guidebook,%20Cybersecurity%20Risk%20Management%20Framework,%20v1.08,%20Sep%202015.pdf](#)
1507
- 1508 Dropping B, Coggins K, Platt J. (2018) Timing Security: Mitigating Threats in a Changing
1509 Landscape Webinar. (ATIS, Washington, DC). Available at [https://www.atis.org/wp-](https://www.atis.org/wp-content/uploads/01_news_events/webinar-pptslides/Timing-Security5222018.pdf)
1510 [content/uploads/01_news_events/webinar-pptslides/Timing-Security5222018.pdf](https://www.atis.org/wp-content/uploads/01_news_events/webinar-pptslides/Timing-Security5222018.pdf)
- 1511 Egea-Roca D, Arizabaleta-Diez M, Pany T, Antreich F, Lopez-Salcedo JA, Paonni M, Seco-
1512 Granados G (2022) GNSS User Technology: State-of-the-Art and Future Trends. *IEEE Access*,
1513 vol. 10, pp.39939–39968. Available at <https://doi.org/10.1109/ACCESS.2022.3165594>
- 1514 Electric Power Research Institute (2020) Roadmap for Resilient Positioning, Navigation, and
1515 Timing (PNT) For the Electricity Subsector. (EPRI, Washington, DC). Available at
1516 <https://www.epri.com/research/products/000000003002020266>
- 1517 European Securities and Markets Authority (2017) Guidelines Transaction Reporting, Order
1518 Record Keeping and Clock Synchronisation Under MiFID II. (EMSA, Lison, Portugal).
1519 Available at [https://www.esma.europa.eu/sites/default/files/library/2016-](https://www.esma.europa.eu/sites/default/files/library/2016-1452_guidelines_mifid_ii_transaction_reporting.pdf)
1520 [1452_guidelines_mifid_ii_transaction_reporting.pdf](https://www.esma.europa.eu/sites/default/files/library/2016-1452_guidelines_mifid_ii_transaction_reporting.pdf)
- 1521 Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White
1522 House, Washington, DC), DCPD-201300091, February 12, 2013. Available at
1523 <https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf>
- 1524 Federal Aviation Administration, Department of Transportation (2020) *NOTAMS, TFRs, Aircraft*
1525 *Safety Alerts* (Department of Transportation, Washington, DC). Available at
1526 https://www.faa.gov/pilots/safety/notams_tfr/
- 1527 Federal Aviation Administration, U.S. Department of Transportation (2020) *Wide Area*
1528 *Augmentation System*. Available at
1529 [https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservice](https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservice/s/gnss/library/factsheets/media/WAAS_QFSheet.pdf)
1530 [s/gnss/library/factsheets/media/WAAS_QFSheet.pdf](https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservice/s/gnss/library/factsheets/media/WAAS_QFSheet.pdf)
- 1531 Federal Aviation Administration, U.S. Department of Transportation (2020) *SBAS Worldwide*.
1532 Available at
1533 [https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservice](https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservice/s/Gnss/library/factSheets/media/SBAS_Worldwide_QFact.pdf)
1534 [s/Gnss/library/factSheets/media/SBAS_Worldwide_QFact.pdf](https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservice/s/Gnss/library/factSheets/media/SBAS_Worldwide_QFact.pdf)
- 1535 Federal Trade Commission (2020) *Jammer Enforcement*. (FCC, Washington, DC). Available at
1536 <https://www.fcc.gov/general/jammer-enforcement>
- 1537 Hopkin P (2018) Fundamentals of risk management: Understanding, evaluating and implementing
1538 effective risk management. Kogan Page Publishers. Available at
1539 [http://dspace.vnbrims.org:13000/xmlui/bitstream/handle/123456789/5077/Fundamentals%20of%20Risk](http://dspace.vnbrims.org:13000/xmlui/bitstream/handle/123456789/5077/Fundamentals%20of%20Risk%20Management.pdf?sequence=1)
1540 [%20Management.pdf?sequence=1](http://dspace.vnbrims.org:13000/xmlui/bitstream/handle/123456789/5077/Fundamentals%20of%20Risk%20Management.pdf?sequence=1)
- 1541 International Maritime Organization (2002) IMO Resolution A.915(22) Revised Maritime Policy
1542 and Requirements for a Future GNSS. (IMO, London, England). Available at

- 1543 [https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/Assembly](https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.915(22).pdf)
1544 [Documents/A.915\(22\).pdf](https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.915(22).pdf)
- 1545 International Organization for Standardization (2018) ISO 31000:2018 – Risk management –
1546 Guidelines (ISO, Geneva, Switzerland). Available at <https://www.iso.org/standard/65694.html>
- 1547 International Organization for Standardization/International Electrotechnical Commission (2018)
1548 ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk
1549 management (ISO, Geneva, Switzerland). Available at <https://www.iso.org/standard/75281.html>
- 1550 Joint Task Force Transformation Initiative (2011) Managing Information Security Risk:
1551 Organization, Mission, and Information System View. (National Institute of Standards and
1552 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
1553 <https://doi.org/10.6028/NIST.SP.800-39>
- 1554 Haimes, Y. Y., Kaplan, S., & Lambert, J. H. (2002). Risk filtering, ranking, and management
1555 framework using hierarchical holographic modeling. *Risk Analysis*, 22(2), 383-397.
- 1556 Lambert JH, Keisler JM, Wheeler WE, Collier ZA, Linkov I (2013). Multiscale approach to the
1557 security of hardware supply chains for energy systems. *Environment Systems and Decisions*, vol.
1558 33 no.3, pp.326-334. Available at <https://doi.org/10.1007/s10669-013-9465-2>
- 1559 Levine J (1999) Introduction to time and frequency metrology. *Review of scientific instruments*
1560 70(6):2567-2596. Available at <https://tf.nist.gov/general/pdf/1288.pdf>
- 1561 Levine J (2016) Measuring Time and Comparing Clocks. (National Institute of Standards and
1562 Technology, Gaithersburg, MD). Available at <https://tf.nist.gov/general/pdf/2718.pdf>
- 1563 [Linkov I, Bridges T, Creutzig F, Decker J, Fox-Lent C, Kröger W, Lambert JH, Levermann A,](#)
1564 [Montreuil B, Nathwani J, Nyer R \(2014\) Changing the resilience paradigm. Nature Climate](#)
1565 [Change. vol.4, no. 6, pp.407-9.](#)
- 1566 National Institute of Standards and Technology (2020) *NIST Time Calibration Services*.
1567 (National Institute of Standards and Technology, Gaithersburg, MD). Available at
1568 <https://www.nist.gov/programs-projects/time-measurement-and-analysis-service-tmas>
- 1569 National Oceanic and Atmospheric Association (2020) *National Geodetic Survey. Antenna*
1570 *Calibrations*. (NOAA, Washington, DC). Available at <https://www.ngs.noaa.gov/ANTCAL/>
- 1571 Nighswander T, Ledvina B, Diamond J, Brumley R, Brumley D (2012) GPS Software Attacks.
1572 *Proceedings of the 2012 ACM Conference on Computer and Communications Security*.
1573 (Association for Computer Machinery, Raleigh, NC), pp. 450-461.
1574 <https://dl.acm.org/doi/10.1145/2382196.2382245>
- 1575 North American Electrical Reliability Corporation (2020) *Reliability Standards for the Bulk*
1576 *Electric Systems of North America, Standard BAL-001-2 – Real Power Balancing Control*
1577 *Performance*. (NERC, Washington, DC). Available at
1578 <https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCCompleteSet>.

- 1579 [pdf](#)
- 1580 Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model:
1581 Prioritizing Systems and Components. (National Institute of Standards and Technology,
1582 Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179.
1583 <https://doi.org/10.6028/NIST.IR.8179>
- 1584 Plumb J, Larson KM, White J, Powers E (2005) Absolute calibration of a geodetic time transfer
1585 system. *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control* 52(11):1904-
1586 11. Available at <https://ieeexplore.ieee.org/abstract/document/1561658>
- 1587 Psiaki M, Humphreys T (2016) GNSS Spoofing and Detection. *Proceedings of the IEEE*, (IEEE,
1588 Piscataway, NJ), pp 1258-1270.
- 1589 Savory J, Sherman J, Romisch S (2018) White rabbit-based time distribution at NIST. *IEEE*
1590 *International Frequency Control Symposium (IFCS)* (IEEE, Piscataway, NJ), pp. 1-5. Available
1591 at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=925954
- 1592 Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control
1593 Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD),
1594 NIST Special Publication (SP) 800-82, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-82r2>
- 1595 Sullivan DB, Allan DW, Howe DA, Walls FL eds. (1990) Characterization of Clocks and
1596 Oscillators. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
1597 Technical Note (TN) 1337. <https://doi.org/10.6028/NIST.TN.1337>
- 1598 University of Texas (2020) *Texas Spoofing Test Battery (TEXBAT)*. (University of Texas,
1599 Austin, TX). Available at
1600 [https://radionavlab.ae.utexas.edu/index.php?option=com_content&view=article&id=289:texas-](https://radionavlab.ae.utexas.edu/index.php?option=com_content&view=article&id=289:texas-spoofing-test-battery-texbat&catid=50&Itemid=27)
1601 [spoofing-test-battery-texbat&catid=50&Itemid=27](https://radionavlab.ae.utexas.edu/index.php?option=com_content&view=article&id=289:texas-spoofing-test-battery-texbat&catid=50&Itemid=27)
- 1602 Lombardi MA (2002) Fundamentals of Time and Frequency. *The*
1603 *Mechatronics Handbook*. Available at <https://tf.nist.gov/general/pdf/1498.pdf>
- 1604 Lombardi MA (2010) A NIST disciplined oscillator: Delivering UTC (NIST) to the calibration
1605 laboratory. *NCSLi Measure* 5(4):46-54. Available at <https://tf.nist.gov/general/pdf/2478.pdf>
- 1606 Lombardi MA, Nelson LM, Novick AN, Zhang VS (2001) Time and Frequency Measurements
1607 Using the Global Positioning System. *Cal. Lab. Int. J. Metrology* July-September:26-33.
1608 Available at <https://tf.nist.gov/general/pdf/1424.pdf>
- 1609 Mader GL (1999) GPS antenna calibration at the National Geodetic Survey. *GPS*
1610 *solutions*3(1):50-8. <https://link.springer.com/article/10.1007/PL00012780>
- 1611 Morton YJ, van Diggelen F, Spilker Jr JJ, Parkinson BW, Lo S, Gao G (2021) Position,
1612 Navigation, and Timing Technologies in the 21st Century, Volumes 1 and 2: Integrated Satellite
1613 Navigation, Sensor Systems, and Civil Applications. (IEEE Press, Piscataway, NJ). Available at

- 1614 <https://ieeexplore.ieee.org/book/9304973>
- 1615 NASPI Time Synchronization Task Force (2017) *Time Synchronization in the Electric Power*
1616 *System. NASPI Technical Report.* (North American Synchrophasor Initiative). Available at
1617 [https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report](https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf)
1618 [_pnnl_26331_march_2017_0.pdf](https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf)
- 1619 National Emergency Number Association (2016) *NENA-STA-026.5 NENA PSAP*
1620 *Master Clock Standard* (NENA, Alexandria, VA). Available at
1621 [https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-STA-](https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-STA-026.5-2016_PSAP_Mas.pdf)
1622 [026.5-2016_PSAP_Mas.pdf](https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-STA-026.5-2016_PSAP_Mas.pdf)
- 1623 National Institute of Standards and Technology (2006) Minimum Security Requirements for
1624 Federal Information and Information Systems. (U.S. Department of Commerce, Washington,
1625 DC), Federal Information Processing Standards Publication (FIPS) 200.
1626 <https://doi.org/10.6028/NIST.FIPS.200>
- 1627 National Institute of Standards and Technology (2020) *NIST Frequency Calibration Services.*
1628 (National Institute of Standards and Technology, Gaithersburg, MD). Available at
1629 <https://www.nist.gov/programs-projects/frequency-measurement-and-analysis-service-fmas>
- 1630 National Institute of Standards and Technology (2020) *NIST Internet Time*
1631 *Service.* (National Institute of Standards and Technology, Gaithersburg, MD).
1632 Available at <https://www.nist.gov/time-distribution/internet-time-service-its>
- 1633 Wang F, Li H, Lu M (2017) GNSS Spoofing Detection and Mitigation Based on Maximum
1634 Likelihood Estimation. *Sensors*, 17:1532.
- 1635 Wong E. (2020) Responsible Use of PNT for DLT in the Financial Services Sector ATIS Time
1636 and Money Conference (New York, NY). Available at
1637 <https://www.gps.gov/multimedia/presentations/2020/ATIS/wong.pdf>
- 1638 Yao J, Lombardi MA, Novick N, Patla B, Sherman JA, Zhang VS. (2016) The Effects of the
1639 January 2016 UTC Offset Anomaly on GPS-Controlled Clocks Monitored At NIST. (National
1640 Institute of Standards and Technology, Gaithersburg, MD.) Available at
1641 <https://tf.nist.gov/general/pdf/2886.pdf>
- 1642 Yao J, Weiss M, Curry C, Levine J (2016) GPS Jamming and GPS Carrier-Phase Time Transfer.
1643 *Proceedings of the 2016 Precise Time and Time Interval Meeting, ION-PTTI 2016* (Monterey
1644 CA), pp 80-85. Available at [https://www.nist.gov/publications/gps-jamming-and-gps-carrier-](https://www.nist.gov/publications/gps-jamming-and-gps-carrier-phase-time-transfer)
1645 [phase-time-transfer](https://www.nist.gov/publications/gps-jamming-and-gps-carrier-phase-time-transfer)

1646 **Appendix D—Applying the PNT Profile to Cybersecurity Risk Management**

1647 The PNT Profile can be used to augment any risk management framework. This section further tailors the PNT Profile in context of a
1648 few fault scenarios. An effective PNT risk management strategy provides a dynamic and flexible approach to control risks in evolving
1649 environments. A comprehensive risk management strategy requires proper preparation, which is further detailed in Appendix E.
1650 Organizations are encouraged to apply the PNT Profile with their risk management framework from concept to acquisitions to
1651 acceptance, integration and deployment, to operations and maintenance.

1652 Each organization selects PNT Profile sub-categories, the cybersecurity outcomes relevant to their mission and business objectives, and
1653 implements associated controls proportional to their risk exposure. The organization verifies and validates the implementation throughout
1654 the PNT system lifecycle. A comprehensive, well-documented, and disciplined risk management process for PNT systems allows for
1655 continuous monitoring of threats, likelihoods, and impacts, in order to provide efficient identification and analysis of risks and
1656 effectiveness of the controls applied to manage those risks. Equally important, an agile risk management approach enables continuous
1657 adaptation to evolving threats through adoption of innovative and rapid advances in technology and current best practices.

1658 Table 25 illustrates how the PNT Profile is used by a notional organization to address example scenarios and apply the five functions of the
1659 CSF to manage the risk to PNT systems.

1660

Table 25 - Applying the PNT Profile to User Risk Management

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

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

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

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

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

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

1661

1662 **Appendix E—Organization Specific PNT Profiles**

1663 NISTIR 8323 provides the foundational set of cybersecurity outcomes based on the five
1664 functions of the NIST Cybersecurity Framework relevant to the responsible use of PNT sources
1665 and data. The set of outcomes selected by the organization based on its mission and business
1666 objectives are intended to manage the risks associated with the use of PNT data. However, it
1667 should be noted that implementation of the foundational profile is necessary but not complete
1668 compliance with Executive Order 13905. This appendix will provide guidance to PNT
1669 stakeholders on applying the NISTIR 8323 to create sector-specific and organization PNT user
1670 profiles and to address other aspects of the Executive Order.

1671 Creating a custom PNT profile based on the foundational profile is beneficial to an organization,
1672 especially if they are part of a critical infrastructure. Each custom PNT profile is intended to
1673 capture the requirements of an organizations PNT source and data and a prioritized set of PNT
1674 data security outcomes. The custom PNT profile can be used to inform new PNT source and
1675 services acquisitions process when researching and evaluating PNT services and sources. In
1676 accordance with EO 13905, the U.S. government will develop contractual language to include
1677 relevant cybersecurity outcomes from the foundational PNT profile as potential requirements in
1678 federal contracts for products, systems, and services that use or integrate PNT services. A custom
1679 profile will facilitate a systematic risk management process for the use of PNT data to meet
1680 sector-specific regulatory and standards requirements. In addition, an organizational PNT profile
1681 would enable assessment of their ability to satisfy the contract when using and providing PNT
1682 sources and data.

1683 Organizations have different assets, architectures, cybersecurity resources and tolerances to PNT
1684 denial or disruption. Accurate, comprehensive, and systematic assessments regarding the
1685 responsible use of PNT requires knowledge of assets, any cybersecurity measures in place,
1686 knowledge of any external dependencies and the impact should there be a loss or degradation of
1687 PNT data that is in the context of the individual organization. Generating the assessment and
1688 definition of a way forward to achieve the appropriate level of PNT assurance will require
1689 leadership and a cadre of subject matter expertise such as:

- 1690 • The Chief Information Officer (CIO). Manages people, processes, and technologies
1691 within the IT organization with the ability to influence the direction of resources for
1692 greater assurance or accept the residual risk.
- 1693 • Cybersecurity Experts. Provides knowledge of cyber-threats and the ability of the current
1694 or proposed IT infrastructure's ability to mitigate attacks.
- 1695 • Operators and Operations Management. Provides knowledge of daily operations and the
1696 impact of an incident or the impact of changes to the IT system on operations.
- 1697 • Users of PNT Data. Provides insight on the impact should the organization's products or
1698 services be delayed, degraded or lost. Provides knowledge of PNT application uses cases
1699 and PNT data performance, reliability, and resilience measures.
- 1700 • System Administration. Configure systems or gather information to provide data for
1701 engineering, analysis or enforce technical and managerial controls.
- 1702 • IT and System Design. Provides knowledge of current or proposed designs and propose
1703 new or modified components or systems.

- 1704 • System Engineering. Integrates modifications or designs of systems providing or
- 1705 transmitting PNT information.
- 1706 • Marketing and Sales Personnel.

1707 Aggregation or easy access to relevant information will expedite the PNT Profile development
1708 process for an organization. This is especially important for the Identify function and will aid in
1709 the ability to evaluate the degree of the organization’s implementation of the categories and
1710 subcategories within all of the functions. The type of information that will be needed will
1711 include:

- 1712 • Any standards, guides, policy, regulations, best practices, concept of operations,
1713 continuity plans, cybersecurity incident response and recovery plans, risk management
1714 documentation, and other documentation that applies to the organization’s business and
1715 mission objectives.
- 1716 • Network and system architecture and diagrams with details such as:
 - 1717 ○ Boundaries
 - 1718 ○ Interfaces
 - 1719 ○ Information flows
 - 1720 ○ Connectivity
 - 1721 ○ Any external dependencies (especially PNT related dependencies)
- 1722 • Network access points to include any temporary access points (such as wireless access
1723 points) or hardware interfaces (such as USB drives, CD’s)
- 1724 • Inventory of assets and their deployment.

1725 Once the team is assembled and the background information is made available, a systematic
1726 analysis of the foundational profile can be made in the context of the individual organization.
1727 Some of the subcategories will require much more robust implementations (relative to other
1728 organizations) while other subcategories may not be as critical.

1729 The organization will have applicable knowledge of their specific protection measures and the
1730 organization’s personnel will provide information that is unique to the organization. As a part of
1731 its findings, the team can provide references, documentation, and other artifacts to supplement
1732 the informative references provided by the Foundational PNT profile. The findings of the team
1733 will enable executives and leaders to make informed decisions regarding the “As is” or
1734 “Proposed” PNT posture.

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

1739

Table 26 - Change Log

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

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

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

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