



Best Practices for Resilient PNT Supporting Critical Infrastructure

September 2024



Science and
Technology

Reference herein to any specific commercial products, processes or services by trade name, trademark, manufacturer or otherwise does not necessarily constitute or imply its endorsement, recommendation or favoring by the U.S. government.

The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the U.S. government.

With respect to documentation contained herein, neither the U.S. government nor any of its employees make any warranty, express or implied, including, but not limited to, the warranties of merchantability and fitness for a particular purpose. Further, neither the U.S. government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed; nor do they

ACKNOWLEDGEMENTS

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the Cybersecurity & Infrastructure Security Agency (CISA) acknowledge and thank all those who have contributed to this guide.

The Homeland Security Systems Engineering & Development Institute (HSSEDI), a Federally Funded Research and Development Center (FFRDC) established by the Secretary of Homeland Security under Section 305 of the Homeland Security Act of 2002. Operated by The MITRE Corporation, HSSEDI aids DHS to develop and maintain the Nation's technical expertise, frameworks and artifacts necessary to guide users, product integrators and supply chain manufacturers on government expectations related to PNT system resilience.

Harold Kiffer Charles Swain Marcus Tamplin Brannan Villee Michael Wilbur Ernest Wong	DHS S&T
Dr. P. Stephen Bedrosian Dr. John Betz Dr. Patricia Larkoski Dr. Bradley Moran J.D. Quartararo Sahar Sadeghian Dr. Shelby Savage Dr. Arthur Scholz	HSSEDI

TABLE OF CONTENTS

Acknowledgements.....	i
List of Figures.....	iii
List of Tables.....	iii
Executive Summary.....	iv
1 Introduction.....	1
1.1 Overview.....	1
1.2 Transitioning from Reliance Solely on GPS.....	2
1.3 Cyclical Implementation of RPNT Best Practices.....	3
2 How to Use This Guide.....	5
2.1 Roles Implementing Resilient PNT Best Practices.....	5
2.2 Additional Resources.....	6
3 Resilient PNT Best Practices.....	8
3.1 Best Practices for Organizational Business Processes, Policies, and Procedures.....	8
3.1.1 Planning and Risk Assessment.....	8
3.1.2 Identify User Needs and Requirements.....	11
3.2 Best Practices for Acquisition of PNT Solutions.....	12
3.2.1 Design, Integrate, and Acquire PNT UE.....	12
3.2.2 Test and Evaluate Equipment.....	20
3.3 Best Practices for Deployment, Operations, and Maintenance.....	22
3.3.1 Deploy and Calibrate.....	22
3.3.2 Operate and Maintain.....	24
4 Conclusion.....	26
Appendix A Definitions.....	27
Appendix B List of Acronyms.....	27
Appendix C References.....	29
Appendix D Index of Best Practices.....	32

LIST OF FIGURES

Relationship of RPNT Best Practices to governance and other documents	1
Cyclical relationship between best practices categories	3
RPNT best practices categories.....	4
Primary responsibilities for stakeholder roles	5
Best Practices for Resilient PNT supporting CI, EO 13905, and related documents.....	6

LIST OF TABLES

Resilient PNT best practices relevant reference summary	7
---	---

EXECUTIVE SUMMARY

The nation's diverse and complex critical infrastructure (CI) systems are vital to maintaining public confidence and the nation's safety, prosperity, and well-being. Recognizing the widespread adoption of Positioning, Navigation, and Timing (PNT) services in CI sectors, this guide aims to provide CI owners and operators, PNT developers, manufacturers, integrators, test labs, and service providers with tailorable best practices for planning, development, and use of PNT systems and services.

The Resilient PNT (RPNT) best practices recommended in this document are organized into categories for the responsible use of PNT services: Organizational Policies (OP), Acquisition of Solutions (AS), and Deployment and Operations (DO). Organizations should assess risk and resilience¹ and use the findings to inform decisions for the responsible use of PNT services in the development, acquisition, and use of PNT technology solutions



The RPNT best practices drive the implementation of the responsible use of PNT across roles:

- **CI Owners** should implement the OP best practices.
- **CI Operators** should implement the DO best practices.
- **PNT UE Manufacturers and Integrators** should implement the AS best practices.
- **Test Equipment Manufacturers and Test Labs** should implement the AS best practices for test and evaluation.
- **PNT Service Providers** should implement the OP best practices and review the AS and DO best practices to understand how they can support downstream users.

All stakeholders have a responsibility to implement the relevant RPNT best practices for their role to enable downstream implementation of related best practices and the responsible use of PNT services.

¹ DHS is sponsoring the development of an RPNT Capability Maturity Model (CM2), which will assist organizations in assessing their RPNT maturity and achieving responsible use of PNT services through risk management, resilience approaches and best practices.

1 INTRODUCTION

1.1 Overview

The nation’s diverse and interdependent critical infrastructure (CI) systems are vital to maintaining public confidence and the nation’s safety, prosperity, and well-being. The *Presidential Policy Directive/PPD-21* (1), and its recent successor *National Security Memorandum/NSM-22* (2) both on *Critical Infrastructure Security and Resilience*, advance a unity of effort to “strengthen and maintain secure, functioning, and resilient critical infrastructure.” *Executive Order 13905* (3), recognizing the widespread adoption of Positioning, Navigation, and Timing (PNT) services in CI sectors, calls for “responsible use of PNT services,” and directs development of PNT profiles that enable the public and private sectors to manage the risks associated with assets that depend on PNT services. The *Foundational PNT Profile* (4) provides guidance for organizations to establish risk management approaches commensurate with acceptable levels of risk.

To support the responsible use of PNT services in CI, this document provides an inclusive guide to PNT best practices for organizational policies, technology solutions, and deployment, operations, and maintenance to implement Resilient PNT (RPNT) solutions. Figure 1 shows how this document supports EO 13905 and draws from a variety of different sources, including the Foundational PNT Profile, to provide guidance at both an organizational level and technology development and operation level. Recognizing different types of risk mitigation for the responsible use of PNT services, this guide organizes the RPNT best practices into categories for organizational business processes, policies, and procedures (OP); acquisitions of

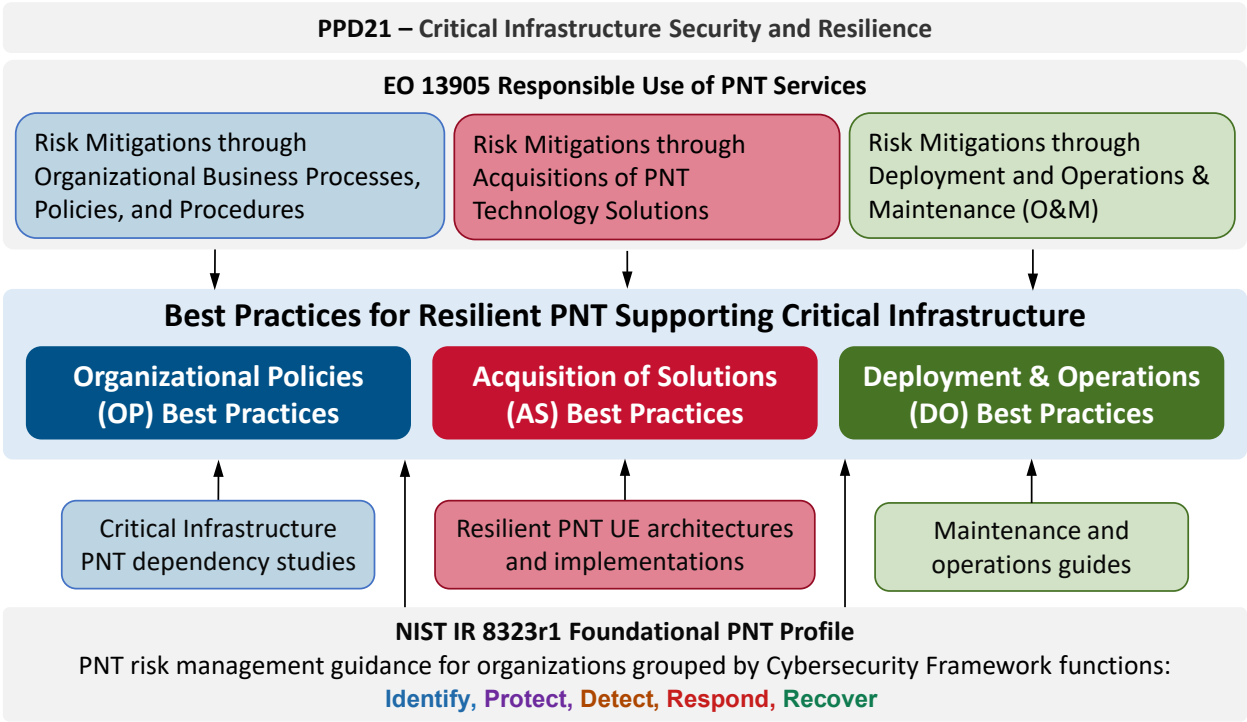


Figure 1. Relationship of RPNT Best Practices to governance and other documents

PNT technology solutions (AS); and deployment, operations, and maintenance (DO), as described in Section 1.3. Each RPNT best practices category can inform the other categories, with assessments from operations and maintenance informing organizational practices, which in turn set the tone for developing and acquiring new equipment to use. Each risk mitigation category, and the implementation of the corresponding best practices, supports the broader context for implementing responsible use of PNT.

The intended audience includes all participants in the implementation of PNT risk mitigation strategies, such as CI owners and operators, PNT UE and test equipment developers and integrators, and service providers (government and commercial providers of PNT services as well as equipment testing services). Not all practices apply to every stakeholder, who should perform judicious tailoring to adapt the contents to the relevant domain.

The RPNT best practices categories are described in more detail in Section 1.3. Section 2.1 provides guidance matching different stakeholder roles to RPNT best practices categories. Section 2.2 provides recommended additional resources relevant for the RPNT best practices in each category. The RPNT best practices are explained in Section 3, and the guide is concluded and summarized in Section 4. The sequential list of best practices provided in the appendix has hyperlinks to the original mention of each numbered practice in the document.

The guide is designed to help readers navigate the best practices, quickly locate relevant guidance, and understand their role within the broader context and the responsible use of PNT. Where possible, this document attempts to provide generalized best practices in principle, illustrated with specific examples that apply to a specific PNT technology (e.g. GPS or GNSS), use case (e.g. stationary timing or moving platform), or role (e.g. PNT service providers or CI owners and operators).

1.2 Transitioning from Reliance Solely on GPS

The unmatched capability of GPS has led to its widespread dependence as a PNT source in the U.S. critical infrastructure and its resulting national security. The ongoing legacy of directly consuming the GPS solution from unsophisticated user equipment (UE) creates fragile reliance, however, which motivates the need for better practices and broader sources. One such recommended practice, known as “The Flip” (5), found in competent UE, uses the GPS solution only to discipline internally integrated components at chosen intervals.

A disciplined architecture logically divides PNT sources into external aiding and local reference categories, the latter of which accumulates error continuously absent the former. Notably the local frequency references, such as Cesium-beam standards, are highly immune to jamming or spoofing and can provide uninterrupted service that bridges aiding gaps during these adversities. If these local references have been previously disciplined, the resulting holdover mode of operation can achieve a defined level of performance depending on the initial state of the reference, the duration of the event, and the quality of the local reference.

Though GPS remains widely used across the nation, alternative PNT sources are available. The U.S. Department of Transportation continuously evaluates complementary PNT sources and

GPS backup technologies (6) and other technologies continue to emerge. This best practices document applies to all current and emerging technologies that provide PNT solutions.

1.3 Cyclical Implementation of RPNT Best Practices

Evolving business practices, emergent PNT threats, and advancing technology solutions illuminate the cyclical nature fundamental to achieving and maintaining PNT resilience for CI systems (2). Figure 2 shows the RPNT best practices categories and subcategories, based on the responsible use of PNT (3), and the notional connections between them. Planning and risk assessment provides the basis for defining user needs and requirements, which in turn drive the design, development, and integration of RPNT UE following the associated best practices. RPNT UE that meets user needs is acquired, tested, and evaluated before it is deployed and calibrated following manufacturer instructions as recommended in the development and evaluation best practices. Deployed equipment is operated and maintained with the associated

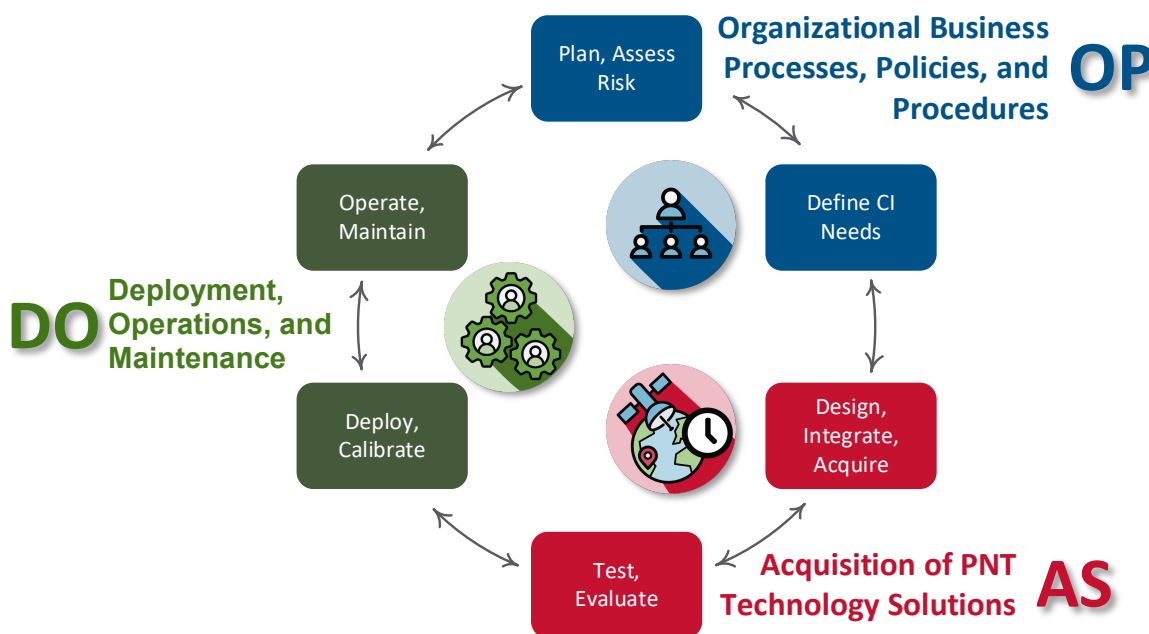


Figure 2. Cyclical relationship between best practices categories

best practices, including logging and anomaly reporting to inform planning and risk assessment, as described in the best practices for periodically updating planning and policy documents. In this way the best practices in each category influence the ability to execute best practices in the connected categories in the depicted cycle.

Every CI application that depends on a PNT service should follow the best practices in all categories, but the associated activities may be spread across one or more institutions and across different organizational levels within each institution. For example, the Acquisition of PNT Technology Solutions best practices may be executed entirely by CI owner/operator staff members or may be completed by external contractors or manufacturers producing RPNT

equipment that is purchased as a turnkey solution. Section 2.1 introduces some of the roles that may execute the different categories of RPNT best practices.

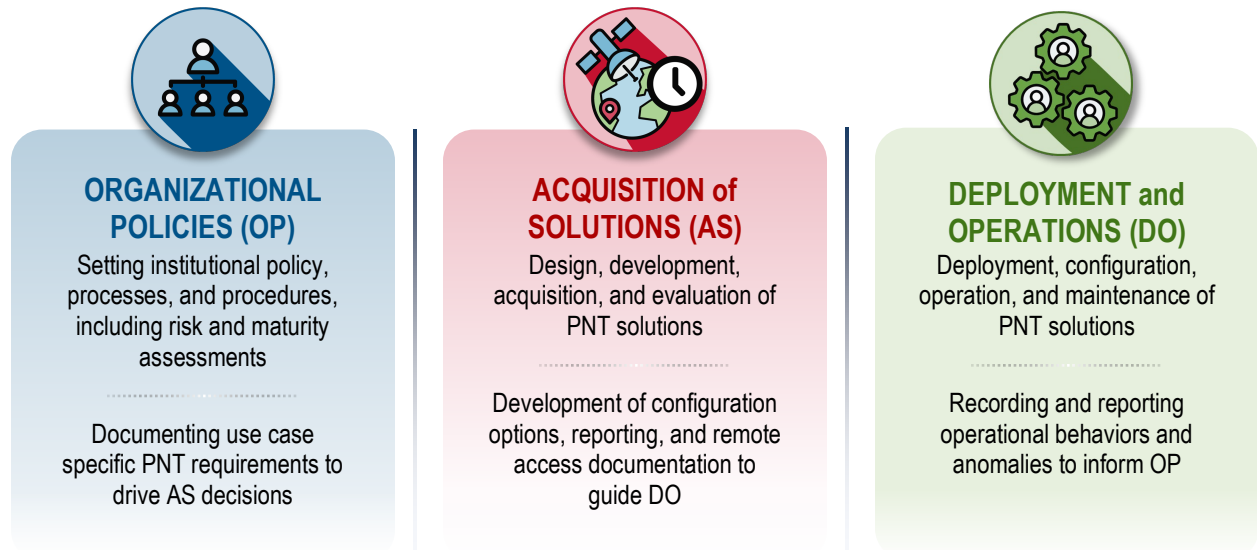


Figure 3. RPNT best practices categories

Figure 3 provides a high-level description of the activities that fall under each RPNT best practices category. Different categories of best practices will be more relevant to different stakeholders.

2 HOW TO USE THIS GUIDE

2.1 Roles Implementing Resilient PNT Best Practices

The intended audience for this document includes all stakeholders with roles that are involved in implementing the responsible use of PNT in CI (Figure 4). In addition to following the primary relevant best practices for their roles, stakeholders should review the connected best practices for familiarity, as shown. For example, the best practices for design and integration of resilient PNT UE inform best practices to identify user needs (including resilient behaviors) and evaluate and deploy the equipment appropriately.




Legend P – primary role responsibility F – familiarity with connected practices	 Organizational Policies	 Acquisition of Solutions	 Deployment and Operations
CI OWNERS set institutional expectations and policies for risk management, security, operations and maintenance; initiate acquisition processes	(P) 3.1	(P) 3.2.1.6 (F) 3.2.1 (F) 3.2.2	(F) 3.3
CI OPERATORS operate and maintain PNT UE, keeping records and providing reports that influence organizational policies and decisions by CI owners			(P) 3.3
UE MANUFACTURERS design, develop, and produce resilient PNT UE per operational needs; document configuration settings for deployment, calibration, and operation of products		(P) 3.2 (F) 3.2.1.6	
INTEGRATORS assemble PNT systems per user needs using COTS components. Integrators may be internal CI personnel, subcontractors that provide integration services, or manufactures with integrated solutions			
TEST EQUIPMENT MANUFACTURERS design, develop, and produce equipment to verify UE compliance; document configuration settings for operation of test equipment		(P) 3.2.2 (F) 3.2.1	(F) 3.3
TEST LABORATORIES evaluate UE using test equipment to ensure performance and resilience			
PNT SERVICE PROVIDERS develop, deploy, operate, and maintain equipment to provide users with a set Quality of Service (QoS)	(P) 3.1	(F) 3.2	(F) 3.3

Figure 4. Primary responsibilities for stakeholder roles

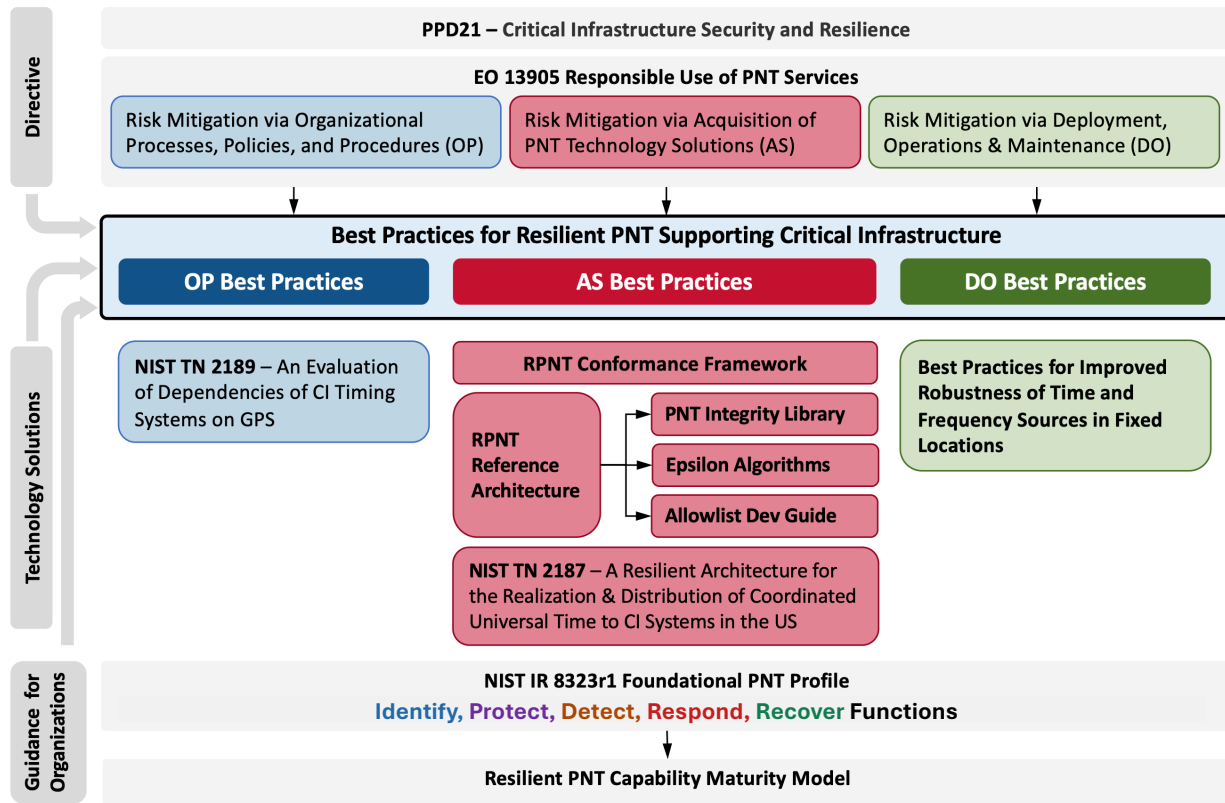


Figure 5. Best Practices for Resilient PNT supporting CI, EO 13905, and related documents




2.2 Additional Resources

This guide and its recommendations fit within an overall context of directives, foundational research, and risk mitigation and resilience philosophies that respond to *PPD-21* (1), *NSM-22* (2) and *EO 13905* (3). The best practices support the responsible use of PNT services with recommendations that apply at the organizational level, encompassing planning and risk assessment, acquisitions, deployment, and operations, as illustrated in Figure 5.

In response to *EO 13905*, the *Foundational PNT Profile* (4) was developed to help organizations integrate PNT considerations into their risk management programs. The *Foundational PNT Profile* provides outcomes and references organized by the five functions defined in the *NIST Cybersecurity Framework* (7): Identify, Protect, Detect, Respond, Recover. DHS S&T is sponsoring development of a Resilient PNT Capability Maturity Model (RPNT CM2), leveraging the *Foundational PNT Profile*, to provide a framework, method and tool to assess maturity and identify outcomes needed to incrementally advance PNT security and resilience within an organization. The RPNT CM2 also draws upon resilience approaches derived from *NIST SP 800-160 Vol. 2 Rev. 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* (8).

Table 1 provides a list of the additional references from Figure 5 mapped to the RPNT best practices categories used to organize Section 3.

Table 1. Resilient PNT best practices relevant reference summary

Resilient PNT Best Practices Category		Relevant References
 OP	Planning & Risk Assessment	<p>NIST IR 8323: <i>Foundational PNT Profile</i> (4) applies the <i>NIST Cybersecurity Framework</i> (9) to provide guidance to organizations managing risks to systems, networks, and assets that use PNT services.</p> <p>NIST TN 2189: <i>An Evaluation of Dependencies of Critical Infrastructure Timing Systems on the Global Positioning System (GPS)</i> (10) contains an overview of timing systems and the dependence of US CI systems in the financial, telecommunications, and electric power sectors on GPS.</p>
	Identify User Needs and Requirements	<p>The <i>Resilient PNT Conformance Framework</i> (11) provides guidance expected behaviors in resilient PNT equipment.</p>
 AS	Design, Integrate, and Acquire PNT UE	<p>The <i>Resilient PNT Reference Architecture</i> (12), incorporating modern cybersecurity principles PNT resilience concepts to provide implementation examples mapped to the <i>Resilient PNT Conformance Framework</i> levels.</p> <p>NIST TN 2187: <i>A Resilient Architecture for the Realization and Distribution of Coordinated Universal Time to CI Systems in the US: Methodologies and Recommendations from NIST</i> (13)</p>
	Test and Evaluate Equipment	<p>See the <i>Resilient PNT Conformance Framework</i> (11)</p>
 DO	Deploy, Calibrate, Operate, and Maintain	<p><i>Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations</i> (16), provides best practices for installation and maintenance of time and frequency sources in fixed infrastructure locations for time & frequency operations.</p>

3 RESILIENT PNT BEST PRACTICES

3.1 Best Practices for Organizational Business Processes, Policies, and Procedures



Business processes, policies, and procedures set the expectations and priorities throughout the organization. These policies should acknowledge the impact of PNT where it is used by the organization and the importance of PNT risk mitigation to downstream applications. Planning, risk assessment, design, testing, retirement, deployment, and operation of PNT components should be included in business processes for product lifecycles.

Organizational leaders who implement the business processes, policies, and procedures are also responsible for coordinating with external stakeholders and reviewing internal processes to ensure that each category of risk mitigation is addressed for the responsible use of PNT in the organization.

The Best Practices in this section have the prefix BP.OP for the Organizational Policies category.

3.1.1 Planning and Risk Assessment

This section focuses on planning activities that support assessments of risk and needs for informed acquisition of PNT equipment/services. Relevant references include the *Foundational PNT Profile* (4) and *Evaluation of Dependencies of CI Timing Systems on GPS* (10), both produced by NIST.

BP.OP.01 Align resilience practices with existing business cycles

System development lifecycles organize business processes and assign roles and responsibilities to stages of planning, risk assessment, design, testing, retirement, deployment, operations, and maintenance. Achieving and maintaining PNT resilience also follows a cycle to adapt to new adversities and incorporate new technology. PNT risk assessments should be included in overall organizational risk assessment processes, policies, and procedures. Equipment installations for CI applications should include PNT UE in overall development lifecycles.

Example Continue to update documentation on CI services and PNT dependencies, external PNT dependencies, and vulnerabilities and reconsider PNT requirements throughout product lifecycles.

BP.OP.02 Perform a maturity assessment to establish a foundation for responsible use of PNT services and inform product lifecycle decisions

Understand the organization's overall PNT maturity posture relative to NIST Cybersecurity Framework functions: Govern, Identify, Protect, Detect, Respond, and Recover. Determine gaps in outcomes to be addressed through the organization's cybersecurity program and implementation of best practices across product lifecycles and other business processes. Identify security and resilience approaches to foster

maturing the organization from foundational, to intermediate, advanced and adaptive levels.

Example Use DHS's RPNT Capability Maturity Model (RPNT CM2) and assessment tool to establish a maturity profile for the organization and develop an action plan to prioritize and address maturity gaps.

BP.OP.03 Inventory existing PNT equipment

Inventory all PNT equipment owned by your organization, including make, model, and software version. Remember that PNT comprises a wide range of hardware and software items, including local clocks, GNSS receivers, beacon receivers, network switches, timing protocol servers, and network interconnections. Based on the criticality and business value of their downstream impact on CI services, build your Prioritize PNT assets list.

BP.OP.04 Assess organizational PNT dependencies and mitigate risk

Understand the nature of organizational PNT service dependencies by examining the existing (or planned) CI architecture and identifying connections, interfaces and PNT service requirements (see also BP.OP.13). Reduce dependencies on external PNT sources where possible.

Example [GPS, TFD] Localized process control and relative ordering of events need not maintain close UTC synchronization such as that typically found using GPS. A local clock can provide sufficient precision with considerably lower risk of disruption, only needing occasional reset to UTC by any number of means, e.g., manual or via Network Time Protocol (NTP).

Example [GPS, TFD] For systems that require precise relative time distributed over a wide area and use GPS provided UTC as an implementation choice, adding complementary sources, including other GNSS, may be an effective risk mitigation to GPS adversities.

BP.OP.05 Maintain awareness of PNT service landscape to initiate new PNT policies when appropriate

Recognize the cyclical nature of achieving and maintaining resilience by monitoring changes in PNT service landscape that warrant initiation of a new PNT policies. This may require changes to internal PNT usage and/or call for external developments, such as new policies, standards, or definitions of emerging PNT threats. If appropriate, set a regular period for reviewing and updating PNT policies.

BP.OP.06 Understand and document dependencies and PNT service guarantees

Identify and document dependencies of critical PNT systems on external PNT sources. Understand expected PNT performance when external PNT sources are unavailable. Document Quality of Service (QoS) guarantees from PNT service providers. Assess the implications of QoS guarantees on the risk for CI PNT users.

BP.OP.07 Advocate for defined limit to GNSS user segment outages

Seek a reasonable guarantee of timely removal of active interference sources that violate spectrum allocations and impact GNSS user equipment. A defined limit

enables risk-informed decision-making based on estimable consequences and practicable solutions to GNSS outages.

Example [GPS] For many use cases an independent clock provides sufficient holdover capability if the federal government can guarantee removal of a localized interference source within 3 days.

BP.OP.08 Establish and Document QoS metrics for downstream users

The performance of PNT technology solutions should be documented for downstream users in the form of comprehensive QoS metrics describing the integrity, accuracy, continuity, area of coverage, and availability of the PNT solution provided to users. Organizations should establish policies to set goals for the PNT QoS provided to users, assess the current QoS metrics, and initiate changes as need to align measured performance with goals.

Example [PNT service providers] Many diverse applications rely on PNT services to meet user PNT needs. PNT service providers need to provide QoS metrics for their services so downstream users, such as CI owners and operators, can develop assess risk and develop appropriate mitigations.

Example [CI owners and operators] To assess risk and implement appropriate mitigations and recovery plans, CI owners and operators should establish the QoS metrics CI use cases can expect from the PNT UE they use. This will depend on the QoS guarantees that have been established for the PNT services the CI PNT UE is dependent on.

BP.OP.09 Understand and document known vulnerabilities

Given the PNT source dependencies identified for BP.OP.06, document the associated known vulnerabilities that can affect those sources. Vulnerabilities may result from local accidents or intentional or unintentional actions, including attacks. The intentional use of jammers, spoofers or cyber infiltrations are examples of attacks, whereas weaknesses in the supply chain or equipment misconfiguration are examples of unintentional adversities.

BP.OP.10 Create response and recovery plans for adverse events

Develop PNT response and recovery plans for adverse events. Ensure a PNT service solution is available for the necessary duration when an adverse event occurs. Ensure systems will fully recover to nominal performance after adverse events. Report adverse events to the relevant authorities (see BP.DO.12 for a list of authorities relevant to different applications).

BP.OP.11 Establish evaluation and maintenance plans

Set policies to continuously evaluate nominal PNT system performance with respect to PNT requirements. Identify parameters to regularly evaluate and determine threshold metrics for detection of PNT anomalies. Establish processes and procedures to regularly evaluate PNT response and recovery plans. Collect PNT UE and PNT service health reports for consideration in maintenance plans.

BP.OP.12 Establish relationships with external stakeholders

Recognize that many threats and hazards, such as radio interference, may originate from sources far from PNT systems and may depend on geopolitical conditions.

Some mitigations thus warrant collaborating with the appropriate authorities/ stakeholders following PNT signal disruption.

Example [GPS] DHS coordinates among federal agencies assigned responsibilities, authorities, and jurisdictions for investigating and mitigating interference with satnav PNT (17).

3.1.2 Identify User Needs and Requirements

Stakeholders from CI owners and operators to manufacturers and integrators should collaborate to identify PNT use case needs, so that CI owners and operators can acquire equipment that meets those needs.

BP.OP.13 Identify relevant PNT performance parameters for user needs

Based on the use case needs and risk tolerance, determine the parameters and acceptable values that specify the required performance of the PNT technology solution. Relevant performance parameters tend to be specific to each use case. For example, they may include accuracy (relative and/or absolute), precision, availability, continuity, stability, area of coverage, assurance, and integrity.

Example [Continuity] When available, use established QoS guarantees from PNT service providers to guide risk management, such as maximum duration of service outage to mitigate via equipment acquisition.

Example [TFD] Ensure that TFD systems support a holdover capability as an independent timing source that can operate with sufficient accuracy for long enough that proper external conditioning can be restored after an incident. Depending on the needs of the PNT use case, different types of local clocks can be used to support the holdover capability.

Example [Positioning] If compatible with the size, weight, power, and cost budget for the use case, positioning or navigation equipment should use inertial sensors for backup when RF signals are unavailable. Coupling between signal tracking and inertial sensors can be loose, tight, or ultra-tight.

BP.OP.14 Identify relevant PNT resilience requirements

Based on the risk tolerance and performance needs, determine the resilience behaviors that are necessary for the use case. PNT resilience requirements can include holdover time (see BP.OP.13), recovery time, allowed performance degradation, and reporting needs. Document adversities that the PNT UE should be prepared to encounter.

Example [IEEE 1952] When the IEEE 1952 standard is complete, it will identify different levels of resilience, the higher of which may require further integration of lower-level components if solutions are not directly available from suppliers. Certification of compliance with IEEE 1952 should be provided by the PNT equipment vendor.

Example [Conformance Framework] The DHS S&T Resilient PNT Conformance Framework provides an initial framework of resilience levels that can be referenced to identify the resilience behaviors required for a use case.

BP.OP.15 Remain aware of regulatory requirements

Stay current regarding regulatory requirements that affect your use of PNT technology.

Example [M-GNSS] Regulatory requirements govern the use of foreign satnav signals. These requirements change, and the Federal Communications Commission (FCC) may grant waivers allowing the use of foreign satnav signals. The only waiver to date was issued in 2018 for the E1 and E5 Galileo signals (18).

3.2 Best Practices for Acquisition of PNT Solutions



CI owners and operators should acquire PNT technology solutions that meet their PNT needs, as defined according to the best practices outlined in Section 3.1.2. Manufacturers and integrators can provide PNT UE products as solutions for these needs. Before deploying new equipment, PNT UE should be evaluated to confirm it meets user requirements. The test industry should collaborate with other stakeholders, including CI owners and operators, manufacturers, integrators, and PNT service providers, to develop tests to appropriately evaluate equipment, using the best practices in Section 3.2.2.

The Best Practices in this section have the prefix BP.AS for the Acquisition of Solutions category.

3.2.1 Design, Integrate, and Acquire PNT UE

Different stakeholders are involved in different types of PNT UE acquisition models. PNT UE can be custom designed and/or integrated or acquired Commercial Off-The-Shelf (COTS) directly from manufacturers. Custom design and/or integration can be performed by employees of CI owners or contracted out to external organizations that provide an integration service. Custom or COTS PNT UE can be acquired by CI owners and operated by CI employee operators or acquired and operated by contract operators that provide a PNT solution service.

The best practices for the designing, integrating, and acquiring PNT UE are grouped together in this section to ensure PNT technology designers and developers follow them when making resilient PNT UE for CI, while CI owners responsible for PNT technology acquisitions should ensure that the PNT UE they purchase conforms to these best practices. Communication and collaboration between stakeholders will enable the successful deployment of PNT technology solutions that meet CI user needs.

3.2.1.1 PNT UE Architecture Best Practices

BP.AS.01 Ensure clear identification of PNT UE dependencies

All dependencies, including necessary services, interfaces, and information sources, should be clearly identified and documented.

Example **[M-GNSS]** Understand how the behavior of PNT UE using foreign satnav changes in the presence of threats. For example, if a Multi-GNSS receiver requires use of one constellation before the other can be used, ensure that performance specifications clearly identify this dependency.

BP.AS.02 Identify appropriate PNT sources

Understand the advantages and risks of different sources of PNT information and determine which sources are appropriate for your use case performance needs and risk tolerance.

Example **[GPS]** Configuring a GPS receiver to use multiple frequency bands can reduce the likelihood of PNT service degradation due to jamming and spoofing directed at any single signal or frequency band. Civil GPS signals include L1 C/A, L1C, L2C, and L5.

Example **[M-GNSS]** Using multiple signals from several satnav constellations can reduce the likelihood of PNT service degradation due to jamming and spoofing directed at any single satnav signal. However, using foreign satnav may not mitigate the entire threat space spectrum. Weigh advantages against the additional cost and complexity that inclusion of such signals may incur. An example analysis of such benefits to specific CI PNT service acquisition strategies is presented in (19).

Example **[Stationary, TFD]** Users should create timing domains to ensure that all clocks in the timing domain are synchronized to the master clock source. The interconnection of Time and Frequency Distribution (TFD) systems forms a timing chain that allows recovery of timing signals at each TFD system in the chain. Communications between TFD systems should use synchronization status messages (SSMs) to ensure the integrity of the timing chain during network rearrangements and faults. The SSMs communicate the clock quality of each TFD system to synchronizing TFD systems in the timing chain, enforce timing distribution rules during reconfiguration, and help to avoid the creation of timing loops. Changes in operating state in a TFD system that result in a lower clock quality may cause synchronizing TFD systems to select other timing inputs or sources that have equal or higher clock quality relative to their internal clock.

BP.AS.03 Identify appropriate holdover or backup capabilities for PNT systems

Holdover or backup capabilities should be selected and used to maintain the required continuity of PNT systems over the necessary duration for your use case when external PNT signals are lost, degraded, or manipulated. When available, use established QoS guarantees from PNT service providers to choose the appropriate equipment (see BP.OP.13).

BP.AS.04 Diversify input sources and signals

Reduce risk by using dissimilar or redundant PNT sources, which allow a system to survive any single point of failure. If feasible and affordable, use PNT sources with separate and diverse characteristics to improve the detection and mitigation of threats. In all cases, analyze PNT systems for common-mode source failures and ensure the PNT services the PNT sources rely on provide appropriate QoS guarantees.

- Example** **[PNT]** Positioning or navigation systems can integrate inertial sensors and proximity sensors to allow continued operation during a temporary outage of satnav [satellite navigation] PNT sources.
- Example** **[GNSS]** Use diverse signal types. For GPS, modernized civil signals (L1C, L2C, and L5) are more robust than the L1 signal and should be leveraged for increased resistance to interference, jamming, and spoofing. There is much less chance that accidental interference will affect all signals on multiple carrier frequencies. Using multiple signals enables jamming and spoofing mitigations (see BP.AS.10 and BP.AS.11). These modern GPS signals also allow forward error control and data demodulation error protection using cyclic redundancy checks, which make data spoofing more difficult. The wider root-mean-square (RMS) bandwidths of L5 and L1C facilitate multipath mitigation, which can also assist in detecting and discriminating against measurement spoofing.
- Example** **[TFD]** TFD systems can use satnav or networked sources and local clocks.
- Example** **[Network Diversity]** Create a timing distribution system that relies on multiple GNSS receivers located at different geographic regions in the network. A downstream timing system can then select one or more of the PNT outputs from these receivers by using one or more selection criteria: (1) select the best input based on synchronization status message signaling; (2) select the best input based on a pairwise comparison of time error – method requires three or more independent sources of timing; (3) if no input source complies with the criteria, the timing system can enter a holdover mode of operation.

BP.AS.05 Develop PNT systems with appropriate redundancy

Robust PNT systems include redundant components to provide backup sources when faults occur. See also the best practices for antenna deployment in Section 3.3.1.

- Example** **[NTP]** Utilize at least two (more than three is strongly recommended) U.S. Naval Observatory (USNO) or NIST-traceable NTP servers from the lowest possible stratum to improve timing accuracy. NTP is a fault-tolerant protocol that automatically selects the best of several available time sources for synchronization based on the NTP clock stratum level. NTP clients can combine multiple input sources to minimize timing error. Even during periods when NTP network sources become temporarily unavailable, the NTP client enters holdover mode during which it uses measurements from the past to estimate current time and time error.

BP.AS.06 Design PNT UE to block undesirable RF inputs upstream

Specialized antennas or situational awareness sensors can limit or block undesirable radio frequency (RF) inputs from reaching a receiver. These specialized antennas can have fixed or adaptive radiation patterns. Situational awareness sensors can detect and characterize aspects of disruptive signals that lead to local anomalies and even cancel out unwanted signals. Blocking unwanted signals limits persistent impact and facilitates handover to backup or holdover devices.

- Example** **[horizon-nulling antennas]** Because jamming and spoofing signals tend to be emitted from the ground, horizon-nulling antennas (also called

blocking antennas) with fixed reception patterns can be used to block unwanted signals. PNT UE algorithms that recognize and reject measurement spoofing (see BP.AS.11) may need adjustment if use in conjunction with a horizon-nulling antenna that reduces the signal power of the threat.

Example [CRPA] Controlled Reception Pattern Antennas (CRPAs) process signals from multiple antenna elements to favor those from expected directions (such as GNSS satellites) and block others.

Example [GPS] A situational awareness sensor can protect a GPS receiver from interference, jamming, or spoofing threats by blocking the RF input when such threats are detected and forcing the system to switch to the holdover device.

BP.AS.07 Develop PNT system architectures that manage trust

Maintain isolation between PNT system components when possible and enforce least privilege access decisions. Seek PNT system architectures that control information across internal and external interfaces based on evaluating trustworthiness, including verification, authentication, validation, and threat detection methods; further information can be found in the *Resilient PNT Reference Architecture* (12) and BP.AS.09, BP.AS.10, and BP.AS.11.

Example [NTP networks] If possible, connect directly to the USNO or NIST NTP servers. To enhance security from threats contained within the firewall, ensure that the time server uses the access control and authentication facilities in NTP to restrict access to the service. If possible, the server should only accept authenticated NTP packets from known, approved sources. When communicating with the time server for status and control, the TFD system should use a secure protocol such as Secure Shell (SSH) and/or Simple Network Management Protocol (SNMP) version 3 (encrypted SNMP).

3.2.1.2 PNT Threat Awareness and Detection

BP.AS.08 Understand relevant threats and ensure PNT equipment has appropriate threat detection and risk mitigation

Employ equipment with the capability to resist PNT service outages during adverse events identified in the risk assessment profile, meeting risk mitigation requirements. Mitigations will depend on the technologies used and the threats of concern in the risk assessment. For example, systems may have a holdover capability to mitigate temporary service disruptions (see BP.AS.03). Also see the anti-jamming and anti-spoofing mitigation examples in BP.AS.10 and BP.AS.11, respectively.

Example [NTP] Take immediate action to ensure that an NTP daemon is not susceptible to use in a reflected denial-of-service (DDOS) attack. NTP is founded on the User Datagram Protocol (UDP) and is highly susceptible to IP spoofing. Block the non-authenticated ports at the firewall to ensure network perimeter security. Refer to the NTP Security Notice site for vulnerability and mitigation details at <http://support.ntp.org/bin/view/Main/SecurityNotice>.

BP.AS.09 Ensure PNT UE has robust input interfaces with conformance verification

Input interfaces should include conformance verification checks to monitor incoming signals and ensure valid message contents. Anomalies can indicate data spoofing. PNT signal monitoring may include allow-listing, integrity verification, authentication, or other signal health checks. All incoming data should be checked before it is stored, used, or output. If conformance verification cannot be implemented at the interface, data can be provided to downstream processors for verification. When illegal or invalid message contents are detected, they should be reported and rejected and appropriate backup or holdover sources of PNT information should be used (see BP.AS.03). Suspicious information should also be recognized and reported. Government reference software that implements allow-list checking should be used to guide implementation and to verify operation of anti-data spoofing.

Example **[GPS]** GPS receivers should conform to the GPS Interface Specification document (IS-GPS-200M) (Global Positioning Systems Directorate Systems Engineering & Integration, “Interface Specification IS-GPS-200M,” 13 April 2021. <https://www.gps.gov/technical/icwg/IS-GPS-200M.pdf>).

Example **[GPS]** See the “GPS Receiver Allow List Development Guide” provided by DHS (20).

BP.AS.10 Develop PNT UE with anti-jam capabilities

PNT UE should be developed with anti-jam capabilities to operate through high received levels of interference and jamming. Techniques to remove unwanted interference or jamming include narrowband excision and signal processing that suppresses constant modulus interference or that estimates and subtracts structured interference or jamming. These techniques can be included in the receiver processing or by adding additional hardware (see BP.AS.06).

Example Adaptive analog-to-digital conversion can provide benefits against some types of interference or jamming.

Example Receivers should use high-sensitivity acquisition processing with long coherent integration times and many noncoherent integrations, along with code Doppler compensation as needed.

Example Robust signal tracking algorithms should be employed using narrow loop bandwidths, including the use of carrier-aided code tracking.

Example **[Stationary]** Stationary timing receivers should be able to use particularly small loop bandwidths once they have acquired signals and initiated tracking. Cross-signal aiding in signal tracking, such as vector-locked loops, can also be used for increased robustness.

Example **[GNSS]** Monitor for significant changes in the RF power and/or for changes in effective C/N_0 .

BP.AS.11 Develop PNT UE with anti-measurement spoof processing

PNT UE should be specified and developed to provide good anti-measurement spoofing—recognizing, rejecting, and reporting spoofing signals that cause the receiver to produce erroneous time of arrival measurements or frequency of arrival measurements. Upon recognition and reporting of spoofing signals, PNT UE should automatically use different sources of PNT information, such as holdover with a

precision clock or inertial sensors (see BP.AS.03). Examples of anti-measurement spoofing techniques include:

- Example** During acquisition, keep the ITU and IFU ranges as small as possible, guided by holdover from high-quality time and frequency sources. Larger ranges can be searched for the presence of spoofing signals.
- Example** Narrow the time and frequency dimensions of tracking loop pull-in regions as tracking loops converge.
- Example** Inspecting position and time outputs using measurements, as available, for anomalous values or changes. Example algorithms can be found in (14) and (15).
- Example** **[GPS]** Calculate and inspect the cross-ambiguity function (CAF) between the input waveform and each true signal to detect the presence of spoofing signals (14). This processing can happen during acquisition and periodically during tracking. This CAF computation should cover the ITU and IFU over which valid signals are expected.
- Example** Implementing multipath mitigation, such as narrow early-late spacing, correlation function shape tests, double-delta and related processing, and multipath-mitigation techniques based on parameter estimation, to discriminate against spoofing signals — even when spoofing signals are spaced close to true signals in delay.
- Example** Measurements from multiple antennas that are spaced on the order of 10 wavelengths apart can be used to detect that different signals are arriving from the same direction, thus are likely to be spoofing signals.
- Example** Inspect RF power levels, reported C/N₀ levels, and/or received signal power levels to identify anomalous values or changes in signal power levels.
- Example** **[Stationary, GPS]** For stationary timing receivers using GPS signals, take advantage of the repeating ground track of GPS satellites to store received power levels from each satellite over time and compare newly received power levels to the reference values. Unless there has been a change or anomaly in the satellite or receive antenna, very tight correspondence should be obtained. Spoofing signals can be detected when they are received at distinctly different signal power levels.
- Example** Combine spoofing mitigation with jamming detection and mitigation (see BP.AS.10). Recognize that sequential or concurrent knockoff jamming can be present with spoofing signals.

3.2.1.3 PNT Management and Output Interfaces

BP.AS.12 Ensure PNT UE has secure configuration interfaces and appropriate documentation

PNT UE should include configurability settings and commands that support initialization and resets (see BP.AS.16). Configuration access should be secure (see BP.AS.17 and BP.DO.09). Examples of configuration options include stationary modes, fixed height, or control over included or excluded signals, constellations, or sensors. Manufacturers should provide instructions to calibrate and configure PNT UE appropriately, including when and how to use different settings and features (see BP.DO.01). Consistency of configuration settings, options, and features across devices facilitates streamlined testing and evaluation (see BP.AS.28).

BP.AS.13 Ensure PNT UE has standard output observables and reporting to enable testing and evaluation

At output interfaces, PNT equipment should provide an adequate set of well-defined observables and state information to enable test and evaluation (see BP.AS.27), which can also support detection of anomalies and monitoring of situational awareness in larger systems or networks. PNT UE should also report at the output anomalies and threats like jamming and spoofing that are detected internal to the equipment.

Example [GNSS] Receivers should capture data when they detect anomalous situations and provide standard output to support analysis. Desired output includes signals tracked, demodulated data message bits, measurements or observables, and RF power levels. Data can be continuously stored in nonvolatile memory then overwritten after several minutes unless an anomaly has occurred. While the capacity may not exist for recording waveform information in a receiver, it may be possible to capture some spectral and power information that could be used to characterize jamming attacks.

Example If a software anomaly is automatically detected and operation is returned to a known good state (see BP.AS.02), the characteristics of this anomaly and other relevant information should be captured and reported.

Example PNT UE should report detected interference, jamming, and spoofing at the output.

BP.AS.14 Enable secure remote access and management for PNT UE

When onsite access and management are not possible or sufficient, it should be possible to securely connect PNT UE to a network for management and information extraction.

Example Enable remote and secure software and firmware updates (see BP.AS.18).

Example Enable secure access to observables and adversity reporting from offsite to enable diagnostics and troubleshooting (see BP.AS.13).

Example Enable remote and secure access to configuration interfaces, including the capability to command reset from offsite when needed (see BP.AS.12).

3.2.1.4 PNT Recovery

BP.AS.15 Ensure PNT UE has adverse event recovery capabilities

PNT systems should support a recovery capability to restore PNT devices to nominal operation and performance after an adverse event. PNT systems may also include automatic recovery capabilities. The UE should allow users to easily upgrade or downgrade firmware or software (see BP.AS.18).

Example [GNSS] If low C/N_0 causes the receiver to lose lock, the receiver should follow prudent steps during reacquisition. For example, it should limit its signal search to as small an initial time uncertainty (ITU), and initial frequency uncertainty (IFU), as possible (guided by high-quality time and frequency information from the holdover device) and perhaps temporarily

use more sensitive thresholds in anti-data spoofing and anti-measurement spoofing as discussed in BP.AS.09 and BP.AS.11. The receiver should scan the entire ITU and IFU, recognizing and reporting the existence of multiple signals having the same spreading code, since such an event likely indicates the presence of spoofing signals.

Example Once interference or jamming has vanished, it can be prudent to delay reacquiring the signal for many minutes or hours, depending on the ability of the holdover source, to reduce the potential for acquiring spoofing signals during reacquisition.

BP.AS.16 Ensure PNT UE has robust reset capabilities

PNT UE should have capabilities to undergo robust reset and to clear portions of volatile or non-volatile memory if needed (see BP.AS.29). Remote reset capabilities allowing the user to command reset without physical access to the PNT UE should be secure (see BP.AS.14).

3.2.1.5 PNT Software and Firmware

BP.AS.17 Ensure PNT UE incorporates software assurance and cybersecurity

All components in PNT devices should have implemented and documented software assurance and cybersecurity practices employed in their design (7). Software should be written so that the processing returns to a known good state either manually by an external command or automatically if the processing is determined to be in an unacceptable state. For example, software should monitor its own operation for situations, such as endless looping, and command a return to a known good state.

BP.AS.18 Plan for software and firmware updates

Ensure all firmware can be updated and software and firmware updates are routinely issued over secure interfaces. Equipment should have the capability to retain a current software version while downloading a new version that can provide bug fixes, enhancements, and defenses against additional threats. When a new software version is installed, there should be a user-selectable time for switchover to that new version, allowing multiple systems to switch over synchronously. The interface for upgrading the software should be nonproprietary, with full open or government-owned documentation. Software upgrade processes should rely on strong authentication, and, in many cases, it may be desirable for upgrades to be enabled only by a physical setting on the unit. Even after an update is installed and enabled, PNT UE should be able to return to the previous software version, if necessary.

BP.AS.19 Plan for growth when developing hardware

Receiver and processor hardware should be architected and designed for adaptability and growth. Ample margin (perhaps at least 50%) should be left in computing resources and storage to accommodate growth in software functionality and size.

3.2.1.6 PNT UE Acquisition

BP.AS.20 Acquire and configure PNT UE to meet use case needs

Buy PNT UE that meets the performance and resilience needs of the use case or application, as defined by planning, risk assessment and requirements best practices (see Section 3.1 Best Practices for Organizational Business Processes, Policies, and Procedures). Configure PNT UE appropriately for the operating conditions and environment.

Example [Stationary, TFD] Use stationary configuration for stationary timing use cases (see BP.AS.12 and BP.DO.01).

Example [GPS] Configure GPS disciplined oscillators to only discipline when needed to maintain the necessary performance parameters for the use case. This limits the opportunity for GPS threats to impact the PNT UE (5).

BP.AS.21 Emphasize trust during procurement

Practice good supply chain hygiene by acquiring equipment from proven and established manufacturers, sources, and service providers when possible.

3.2.2 Test and Evaluate Equipment

The PNT test industry, including test equipment manufacturers and test labs, should provide leadership for the PNT test and evaluation best practices. They should engage with PNT CI owners and operators and PNT UE manufacturers to ensure testing and evaluation provides the necessary information to users and suitably demonstrates PNT UE capabilities. *The Resilient PNT Conformance Framework* (11), produced by DHS S&T, provides additional guidance for testing and evaluation of resilient behavior requirements for PNT UE.

The PNT test industry, including test equipment manufacturers and test labs, should provide leadership for the PNT test and evaluation best practices. They should engage with PNT CI owners and operators and PNT UE manufacturers to ensure testing and evaluation provides the necessary information to users and suitably demonstrates PNT UE capabilities.

BP.AS.22 Create test plans for foreseeable adverse PNT events

Produce plans for qualification and testing to evaluate PNT UE performance during known or foreseeable adverse events (e.g., UTC [Coordinated Universal Time] leap seconds or GPS week number rollovers).

BP.AS.23 Define example PNT UE test suites for reference by manufacturers, evaluators, procurers, and operators

This should include PNT UE test methods, terminology, and metrics, as well as documentation sufficient for reproducibility.

BP.AS.24 Ensure evidence of testing threat protections are made available to the user

Ensure evidence of threat testing and protections are made available to the user, including validation of anti-jam and anti-spoof capabilities, as well as foreseeable adverse events (see BP.AS.22).

BP.AS.25 Ensure PNT UE has qualified performance specifications

In addition to typical performance metrics in nominal conditions, ensure performance metrics are provided for adverse operating conditions, including threat and disruption situations when one or more external PNT sources may not be available. When using multiple PNT services, ensure that specifications for each clarify performance with and without supplemental sources.

Example [M-GNSS] For example, if a Multi-GNSS receiver uses GPS and Galileo constellations, specify the necessary performance with (1) both constellations available, and (2) each constellation available separately.

BP.AS.26 Create test equipment for extended PNT use cases

Use cases vary by PNT source and type of PNT UE. The baseline test equipment covers nominal PNT performance under relevant use cases. Subcategories of the baseline may include (1) varying Position, Velocity, and Time (PVT) sources (e.g., sources from GNSS constellations and other sensors), (2) PNT outputs and dynamics (e.g., PVT vs. timing only, or stationary vs. moving), (3) PNT signal availability, and (4) PNT UE operating modes and initialization. In addition to testing nominal performance, test equipment can enable extended use cases, including:

Example [ICD compliance] This category focuses on likely areas of non-compliance, including PNT interfaces (e.g., GNSS and other PVT sources) and non-PNT interfaces (e.g., serial/USB [universal serial bus], Ethernet, Wi-Fi, and Bluetooth). It includes rare or problematic events and data validation. Examples of past GPS non-compliance with Interface Control Documents (ICDs) and resulting adverse events include rollovers in week number and epoch, UTC leap second adjustments, and use of the issue-of-data-and-clock upper range. Data validation includes evaluation of allowlisting (formerly called whitelisting), bounds checking, and exception handling for values, states, and valid ranges, as defined in relevant standards and ICDs.

Example This category includes targeted and non-targeted testing. Targeted testing may be based on Common Vulnerability Enumeration (CVE) and similar vulnerability databases and Common Weakness Enumeration (CWE). Non-targeted testing may involve fuzzing or protocol-constrained, randomized inputs.

Example This category introduces RF interference into testing of nominal performance to evaluate the impact on PVT performance, availability, and resilience. Testers may select waveforms representative of intentional or unintentional jamming.

Example [GPS] UE spoofing attacks include the transmission of false GPS signals with incorrect navigation data or manipulated signal delays. They can also include false aiding signals, such as network timing sources and assisted GPS systems such as the Wide Area Augmentation Service (WAAS). RF spoof signals may be accompanied by jamming attacks that cause GPS

receivers to lose signal tracking, forcing them to accidentally reacquire spoofing signals.

BP.AS.27 Ensure observables relevant to PNT UE testing are provided over output interfaces

Useful observables include PNT signals tracked, inputs used in output formulation (e.g. data messages), QoS metrics such as RF channel power, automatic gain controls, and pseudo-ranges. Signal-to-noise and carrier-to-noise ratios are particularly useful, provided testers use the correct definition and estimation methods (21). See BP.AS.13 for PNT UE design considerations regarding output observables.

BP.AS.28 Seek consistency of and documentation of PNT UE operational modes, settings, and features to support improved testing, automation, and resilience

Because of differences in applications, requirements, and technology, different types of PNT UE necessarily vary in modes, settings, and features; for example, stationary modes may be appropriate for some timing receivers (see BP.AS.12 and BP.DO.01), while other receivers may include options for fixed height or control over included or excluded sources, such as individual signals, constellations, or sensors. Additional enhancements may include anti-jam and anti-spoof capabilities or automatic gain control (AGC). Users and evaluators should follow manufacturer instructions to determine when to enable or disable certain features and should understand the associated considerations and tradeoffs. Evaluators should document all configuration settings used during testing.

BP.AS.29 Seek consistency of and documentation of resets, programmability, and initialization

Document demonstrated PNT UE capabilities to undergo robust reset and to clear portions of volatile or non-volatile memory (see BP.AS.16). Confirm the ability to easily upgrade or downgrade PNT UE firmware or software (see BP.AS.18). Seek standardization of ways to initialize necessary data, modes, and settings to facilitate testing and streamline evaluation procedures.

3.3 Best Practices for Deployment, Operations, and Maintenance



This section focuses on deployment, operations, and maintenance of PNT user equipment. End users should follow site-specific instructions pertaining to topics such as placement of PNT signal antennas. This section further covers operations and maintenance procedures to use the PNT UE as intended.

The Best Practices in this section have the prefix BP.DO for the Deployment and Operations category.

3.3.1 Deploy and Calibrate

Manufacturers should prepare instructions for site adaptation and calibration procedures. These instructions should be implemented when PNT UE is deployed. *Best Practices for Improved*

Robustness of Time and Frequency Sources in Fixed Locations (16), is an additional resource providing detailed instructions for installation and maintenance of time and frequency sources in fixed infrastructure locations for time and frequency operations.

BP.D0.01 Use appropriate, site-specific, configuration settings and calibrate equipment

Ensure configuration settings consistent with the use case conditions are selected, following manufacturer documentation for the PNT UE (see BP.AS.12). All equipment should be calibrated following manufacturer instructions to compensate for site-specific characteristics.

Example **[GNSS]** Through specifications or measurements, determine the delay characteristics of GNSS antennas, cables, and antenna electronics, making sure the bulk delay is small enough for a timing receiver to compensate for the delay. Evaluate delay variations—whether due to thermal effects, aging in fixed pattern antennas and their electronics, and/or the effects of adaptive anti-jam antennas and their electronics—and ensure they meet accuracy requirements.

Example **[Stationary, TFD, GNSS]** Operate stationary GNSS timing receivers in position hold mode when available, making sure they are properly installed and configured (surveyed) to function correctly in this mode. In this mode, they must receive signals from only one satellite to provide timing measurements. If the receiver uses timing receiver autonomous integrity monitoring (TRAIM), determine how many satellites the receiver requires for TRAIM and how the receiver behaves if it does not receive signals from the customary number of satellites. If the option exists, use a receiver that operates with only high-elevation satellites, even if it cannot then support TRAIM.

BP.D0.02 Carefully select antenna locations

Install PNT signal antennas >10 m away from (and at least slightly above) nearby structures to ensure that the local multipath environment is benign and antenna beam patterns are not distorted. Choose a location where the antenna has an adequate view of the sky. Consider hazards such as birds and lightning/inclement weather in site selection.

Example **[Stationary, TFD, GPS]** For stationary timing GPS receivers, place antennas so that they have a clear view of the sky in at least a $\pm 30^\circ$ sector around vertical at all azimuth angles. Simultaneously, seek locations where roof lines or other structures block RF propagation from the ground and other publicly accessible locations.

BP.D0.03 Obfuscate visibility of the primary antenna

Install PNT signal antennas at sites not visible from publicly accessible locations or obscure their exact locations to mitigate tampering, disruption, and deception. When feasible, at an appropriate distance from the primary, add one or more secondary (decoy) antennas connected to a situational awareness sensor.

Example **[GPS, M-GNSS]** Conceal antenna locations with optically opaque but electromagnetically transparent barriers.

Example [GPS] Decoy GPS antenna separation should exceed the length of a coarse acquisition (C/A) signal chip, namely 300 m.

BP.DO.04 Avoid the reception of low-elevation PNT RF signals where possible

Especially when using horizon-nulling PNT antennas (see BP.AS.06), ensure that timing receivers do not use measurements from low-elevation (e.g., $< 25^\circ$) satellites, since those signals are attenuated by the horizon-nulling antennas. Even if horizon nulling-antennas are not used, consider the benefits of excluding measurements taken at lower elevation angles, since they usually have poorer quality—signals generally received at lower power and more strongly degraded by ground interference and other propagation phenomena.

3.3.2 Operate and Maintain

Once PNT UE has been deployed and calibrated, operators should follow operations and maintenance procedures, including monitoring for and reporting anomalies. Fixed infrastructure locations using PNT UE for time and frequency operations can find additional detailed guidance in *Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations* (16).

BP.DO.05 Monitor for outages in PNT infrastructure services

Because many PNT systems, such as GPS receivers, use infrastructure outside the user's control, document QoS guarantees and dependencies and set up an alert system to remain informed of potential or scheduled outages or degraded services from PNT service providers.

BP.DO.06 Automate detection of adverse PNT events

Design data flows to and from PNT equipment to support the detection and reporting of adverse PNT events and conditions. Employ automatic fault detection and alerts, using detection thresholds determined by tests of nominal and anomalous data. When possible, use designs that incorporate multiple PNT sensors, which supports the direct comparison of PNT signals, since disagreements between PNT systems may indicate adverse events. Monitor the environment according to sensor type and use case.

BP.DO.07 Appropriately manage identities and credentials

Enforce use of appropriate identification and authentication credentials for PNT users, PNT applications, and data sources to ensure proper use of resources and integrity of data, and revoke credentials when users no longer need access. Assess the effects of authentication and encryption protocols, because, for example, processing delays can affect PNT services, which often depend on real-time processing.

BP.DO.08 Maintain PNT system software and securely update firmware when needed

PNT UE is commonly implemented as software systems with an assortment of interfaces and network connections; therefore, firmware and/or software should be securely updated throughout the product lifecycle.

BP.DO.09 Practice good cyber hygiene

Follow good cyber hygiene practices, since both the GPS receiver and any associated processors are computers (often networked). Install and maintain firewalls, virus protection, and other defenses, such as protections applied to any other mission-critical computing system. Authenticate software patches and updates and then apply them promptly. Require two-factor authentication, including strong passwords, for access. Change all factory default and maintenance passwords and update them regularly. If continuous network connectivity is unnecessary, it may be prudent to operate without a network connection except when such a connection is needed.

BP.DO.10 Assess PNT UE operational performance

Maintain logs of operational PNT UE performance. Operators and maintainers serve as the front line for evaluating the compliance of PNT UE serving CI and provide key inputs to update and improve organizational policies and procedures regarding PNT.

BP.DO.11 Keep PNT UE audit logs in compliance with regulations and legal requirements

Maintain audit logs, using existing standard data formats where possible and including identities of individuals and components that may be affected by adverse events. PNT applications with an audit trail sometimes require legal or metrological traceability (22; 23; 24; 25; 26).

BP.DO.12 Report suspicious PNT UE events and adverse conditions to appropriate authorities

The public and private sectors operate systems that collect information on the availability and performance of widely adopted PNT UE. These data are invaluable in identifying and responding to service outages.

Example The Navigation Center (<https://www.navcen.uscg.gov/home>) is the U.S. Coast Guard's center of excellence for systems and policy related to electronic PNT. This includes radionavigation, electronic charting, and vessel identification and tracking.

Example The Aviation Safety Reporting System (<https://asrs.arc.nasa.gov/>) captures confidential reports, analyzes the resulting aviation safety data, and disseminates vital information to the aviation community.

Example The Electricity Information Sharing and Analysis Center (<https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>) gathers and analyzes security data, shares appropriate data with stakeholders, coordinates incident management, and communicates mitigation strategies with stakeholders.

Example The Network Time Foundation (NTF) provides direct services and support to improve the state of accurate computer network timekeeping. NTF's flagship effort is the Network Time Protocol Project, used by almost every networked computer in the world. NTP Security Information (https://support.ntp.org/Main/WebHome#NTP_Security_Information) states that security-related bugs, confirmed or suspected, should be reported by email (security@ntp.org).

4 CONCLUSION

The above best practices represent guidelines relevant at the time of writing based on widely adopted PNT technology solutions and PNT services used in CI sectors. CI owners and operators, manufacturers, integrators, test labs, and service providers should devote ongoing efforts to monitoring, assessing and evaluating new guidance, and/or changes to existing guidance necessitated by emerging PNT technologies.

APPENDIX A DEFINITIONS

PNT service	Executive Order 13905 defines a PNT service as “any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof” (3)
PNT source	A source of PNT information. PNT sources can be local references, such as local clocks or inertial sensors, or external aiding sources, providing signals received from outside the physical bounds of the PNT UE. Examples of external sources include GNSS or LEO satellites transmitting PNT signals.
PNT solution	The PNT information product provided to PNT users to meet application needs. The PNT solution will be one or more components of position, velocity, acceleration, orientation, time, and/or frequency.
PNT technology solution, PNT user equipment (PNT UE), PNT system	Synonyms for implementation of PNT technology in the form of deployed equipment that provides a PNT solution to PNT users, using information from PNT sources
PNT user	A consumer of a PNT solution. PNT users may be people, subsystems, or application components.

APPENDIX B LIST OF ACRONYMS

AGC	Automatic Gain Control
C/A	Coarse Acquisition
CI	Critical Infrastructure
CF	Conformance Framework
COTS	Commercial-off-the-Shelf
CVE (CWE)	Common Vulnerability (Weakness) Enumeration
DHS	Department of Homeland Security
E-ISAC	Electricity Information Sharing and Analysis Center
EO	Executive Order
FCC	Federal Communications Commission
FFRDC	Federally Funded Research and Development Center
GNSS, M_	Global Navigation Satellite System (Multi-)
GPS	Global Positioning System
HSSEDI	Homeland Security Systems Engineering & Development Institute
ICD	Interface Control Document
IS	Interface Specification
NASA	National Aeronautics and Space Administration
NAVCEN	U.S. Coast Guard Navigation Center
NERC	North American Electrical Reliability Corporation
NIST	National Institute of Standards and Technology
PPD	Presidential Policy Directive
PNT (RPNT)	Positioning, Navigation, and Timing (Resilient PNT)
PTP	Precision Time Protocol

PVT	Position, Velocity, Time
QoS	Quality of Service
RA	Reference Architecture
RF	Radio Frequency
RPNT CM2	Resilient PNT Capability Maturity Model
TFD	Time and Frequency Distribution
TRAIM	Timing Receiver Autonomous Integrity Monitoring
UE	User Equipment
USNO	United States Naval Observatory
UTC	Coordinated Universal Time
WAAS	Wide Area Augmentation Service

APPENDIX C REFERENCES

1. **The President of the United States.** Presidential Policy Directive -- Critical Infrastructure Security and Resilience. Washington, DC : The White House, 2013. PPD-21.
2. —. National Security Memorandum on Critical Infrastructure Security and Resilience. Washington, DC : The White House, 2024. NSM-22.
3. —. Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services. Washington, DC : Executive Office of the President, 2020. EO 13905
4. **National Institute of Standards and Technology.** *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services.* Gaithersburg, MD : U.S. Department of Commerce, 2023. NIST IR 8323 Rev. 1.
5. **Betz, John.** *Achieving Robust and Resilient Navigation and Timing for Defense Applications.* McLean, VA : The MITRE Center for Technology and National Security, 2019.
6. **Hansen, A., et al.** *Complementary PNT and GPS Backup Technologies Demonstration Report.* Cambridge, MA : U.S. Department of Transportation Volpe Center, 2021.
7. **National Institute of Standards and Technology.** *The NIST Cybersecurity Framework 2.0.* Gaithersburg, MD : U.S. Department of Commerce, 2023.
8. —. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.* Gaithersburg, MD : U.S. Department of Commerce, 2021.
9. —. *Framework for Improving Critical Infrastructure Cybersecurity.* Gaithersburg, MD : U.S. Department of Commerce, 2018.
10. **Lombardi, Michael A.** *An Evaluation of Dependencies of Critical Infrastructure Timing Systems on the Global Positioning System (GPS).* Gaithersburg, MD : National Institute of Standards and Technology, 2021. Technical Note (NIST TN) - 2189.
11. **Homeland Security Science and Technology.** *Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework.* Washington, DC : U.S. Department of Homeland Security, 2022.
12. —. *Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture.* Washington, DC : U.S. Department of Homeland Security, 2022.
13. **National Institute of Standards and Technology.** *A Resilient Architecture for the Realization and Distribution of Coordinated Universal Time to Critical Infrastructure Systems in the United States.* Gaithersburg, MD : NIST, 2021.

14. **Integrated Solutions for Systems, Inc.** PNT Integrity Library. *Cybersecurity and Infrastructure Security Agency - GitHub*. [Online] U.S. Department of Homeland Security, 2021. <https://github.com/cisagov/PNT-Integrity>.
15. **Homeland Security Systems Engineering and Development Institute (HSSEDI)**. Epsilon Algorithm Suite. *Cybersecurity and Infrastructure Security Agency - GitHub*. [Online] U.S. Department of Homeland Security, 2021. <https://github.com/cisagov/Epsilon>.
16. **Cybersecurity and Infrastructure Security Agency (CISA)**. *Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations*. Washington, DC : U.S. Department of Homeland Security, 2015.
17. **U.S. Department of Homeland Security**. *United States Positioning, Navigation, and Timing Interference Detection and Mitigation Plan Summary*. Washington, D.C. : U.S. Department of Homeland Security, 2008.
18. **National Coordination Office for Space-Based Positioning, Navigation, and Timing**. GPS.gov: Use of Foreign Satellite Navigation Signals. [Online] Oct 19, 2021. <https://www.gps.gov/spectrum/foreign/>.
19. **Homeland Security Systems Engineering and Development Institute (HSSEDI)**. *Multi-GNSS Assessment Report*. Washington, DC : U.S. Department of Homeland Security, 2022.
20. **Homeland Security Science and Technology**. *GPS Receiver Allow List Development Guide*. Washington, D.C. : U.S. DHS, 2021.
21. **National Cybersecurity & Communications Integration Center, National Coordinating Center for Communications**. *Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure*. Washington, D.C. : U.S. Department of Homeland Security, 2017.
22. **Cybersecurity and Infrastructure Security Agency (CISA)**. *Time Guidance for Network Operators, Chief Information Officers, and Chief Information Security Officers*. Washington, D.C. : U.S. Department of Homeland Security, 2020.
23. **Matsakis, D, Levine, J and Lombardi, M**. *Metrological and legal traceability of time signals*. Gaithersburg, Maryland : National Institute of Standards and Technology, 2018.
24. **Ross, R, et al**. *Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*. Gaithersburg, MD : National Institute of Standards and Technology, 2018.
25. **Joint Task Force Transformation Initiative**. *Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, Maryland : National Institute of Standards and Technology, 2020.

26. **Committee on National Security Systems.** *Committee on National Security Systems (CNSS) Glossary.* Ft. Meade, MD : CNSS Secretariat, 2015.

APPENDIX D INDEX OF BEST PRACTICES

BP.OP.01 Align resilience practices with existing business cycles.....8

System development lifecycles organize business processes and assign roles and responsibilities to stages of planning, risk assessment, design, testing, retirement, deployment, operations, and maintenance. Achieving and maintaining PNT resilience also follows a cycle to adapt to new adversities and incorporate new technology. PNT risk assessments should be included in overall organizational risk assessment processes, policies, and procedures. Equipment installations for CI applications should include PNT UE in overall development lifecycles.

BP.OP.02 Perform a maturity assessment to establish a foundation for responsible use of PNT services and inform product lifecycle decisions.....8

Understand the organization’s overall PNT maturity posture relative to NIST Cybersecurity Framework functions: Govern, Identify, Protect, Detect, Respond, and Recover. Determine gaps in outcomes to be addressed through the organization’s cybersecurity program and implementation of best practices across product lifecycles and other business processes. Identify security and resilience approaches to foster maturing the organization from foundational, to intermediate, advanced and adaptive levels.

BP.OP.03 Inventory existing PNT equipment.....9

Inventory all PNT equipment owned by your organization, including make, model, and software version. Remember that PNT comprises a wide range of hardware and software items, including local clocks, GNSS receivers, beacon receivers, network switches, timing protocol servers, and network interconnections. Based on the criticality and business value of their downstream impact on CI services, build your Prioritize PNT assets list.

BP.OP.04 Assess organizational PNT dependencies and mitigate risk9

Understand the nature of organizational PNT service dependencies by examining the existing (or planned) CI architecture and identifying connections, interfaces and PNT service requirements (see also BP.OP.13). Reduce dependencies on external PNT sources where possible.

BP.OP.05 Maintain awareness of PNT service landscape to initiate new PNT policies when appropriate9

Recognize the cyclical nature of achieving and maintaining resilience by monitoring changes in PNT service landscape that warrant initiation of a new PNT policies. This may require changes to internal PNT usage and/or call for external developments,

such as new policies, standards, or definitions of emerging PNT threats. If appropriate, set a regular period for reviewing and updating PNT policies.

BP.OP.06 Understand and document dependencies and PNT service guarantees9

Identify and document dependencies of critical PNT systems on external PNT sources. Understand expected PNT performance when external PNT sources are unavailable. Document Quality of Service (QoS) guarantees from PNT service providers. Assess the implications of QoS guarantees on the risk for CI PNT users.

BP.OP.07 Advocate for defined limit to GNSS user segment outages9

Seek a reasonable guarantee of timely removal of active interference sources that violate spectrum allocations and impact GNSS user equipment. A defined limit enables risk-informed decision-making based on estimable consequences and practicable solutions to GNSS outages.

BP.OP.08 Establish and Document QoS metrics for downstream users 10

The performance of PNT technology solutions should be documented for downstream users in the form of comprehensive QoS metrics describing the integrity, accuracy, continuity, area of coverage, and availability of the PNT solution provided to users. Organizations should establish policies to set goals for the PNT QoS provided to users, assess the current QoS metrics, and initiate changes as need to align measured performance with goals.

BP.OP.09 Understand and document known vulnerabilities 10

Given the PNT source dependencies identified for BP.OP.06, document the associated known vulnerabilities that can affect those sources. Vulnerabilities may result from local accidents or intentional or unintentional actions, including attacks. The intentional use of jammers, spoofers or cyber infiltrations are examples of attacks, whereas weaknesses in the supply chain or equipment misconfiguration are examples of unintentional adversities.

BP.OP.10 Create response and recovery plans for adverse events 10

Develop PNT response and recovery plans for adverse events. Ensure a PNT service solution is available for the necessary duration when an adverse event occurs. Ensure systems will fully recover to nominal performance after adverse events. Report adverse events to the relevant authorities (see BP.DO.12 for a list of authorities relevant to different applications).

BP.OP.11 Establish evaluation and maintenance plans 10

Set policies to continuously evaluate nominal PNT system performance with respect to PNT requirements. Identify parameters to regularly evaluate and determine

threshold metrics for detection of PNT anomalies. Establish processes and procedures to regularly evaluate PNT response and recovery plans. Collect PNT UE and PNT service health reports for consideration in maintenance plans.

BP.OP.12 Establish relationships with external stakeholders..... 10

Recognize that many threats and hazards, such as radio interference, may originate from sources far from PNT systems and may depend on geopolitical conditions. Some mitigations thus warrant collaborating with the appropriate authorities/ stakeholders following PNT signal disruption.

BP.OP.13 Identify relevant PNT performance parameters for user needs 11

Based on the use case needs and risk tolerance, determine the parameters and acceptable values that specify the required performance of the PNT technology solution. Relevant performance parameters tend to be specific to each use case. For example, they may include accuracy (relative and/or absolute), precision, availability, continuity, stability, area of coverage, assurance, and integrity.

BP.OP.14 Identify relevant PNT resilience requirements 11

Based on the risk tolerance and performance needs, determine the resilience behaviors that are necessary for the use case. PNT resilience requirements can include holdover time (see BP.OP.13), recovery time, allowed performance degradation, and reporting needs. Document adversities that the PNT UE should be prepared to encounter.

BP.OP.15 Remain aware of regulatory requirements 12

Stay current regarding regulatory requirements that affect your use of PNT technology.

BP.AS.01 Ensure clear identification of PNT UE dependencies 12

All dependencies, including necessary services, interfaces, and information sources, should be clearly identified and documented.

BP.AS.02 Identify appropriate PNT sources 13

Understand the advantages and risks of different sources of PNT information and determine which sources are appropriate for your use case performance needs and risk tolerance.

BP.AS.03 Identify appropriate holdover or backup capabilities for PNT systems 13

Holdover or backup capabilities should be selected and used to maintain the required continuity of PNT systems over the necessary duration for your use case when external PNT signals are lost, degraded, or manipulated. When available, use

established QoS guarantees from PNT service providers to choose the appropriate equipment (see BP.OP.13).

BP.AS.04 Diversify input sources and signals 13

Reduce risk by using dissimilar or redundant PNT sources, which allow a system to survive any single point of failure. If feasible and affordable, use PNT sources with separate and diverse characteristics to improve the detection and mitigation of threats. In all cases, analyze PNT systems for common-mode source failures and ensure the PNT services the PNT sources rely on provide appropriate QoS guarantees.

BP.AS.05 Develop PNT systems with appropriate redundancy 14

Robust PNT systems include redundant components to provide backup sources when faults occur. See also the best practices for antenna deployment in Section 3.3.1.

BP.AS.06 Design PNT UE to block undesirable RF inputs upstream 14

Specialized antennas or situational awareness sensors can limit or block undesirable radio frequency (RF) inputs from reaching a receiver. These specialized antennas can have fixed or adaptive radiation patterns. Situational awareness sensors can detect and characterize aspects of disruptive signals that lead to local anomalies and even cancel out unwanted signals. Blocking unwanted signals limits persistent impact and facilitates handover to backup or holdover devices.

BP.AS.07 Develop PNT system architectures that manage trust..... 15

Maintain isolation between PNT system components when possible and enforce least privilege access decisions. Seek PNT system architectures that control information across internal and external interfaces based on evaluating trustworthiness, including verification, authentication, validation, and threat detection methods; further information can be found in the *Resilient PNT Reference Architecture* (12) and BP.AS.09, BP.AS.10, and BP.AS.11.

BP.AS.08 Understand relevant threats and ensure PNT equipment has appropriate threat detection and risk mitigation..... 15

Employ equipment with the capability to resist PNT service outages during adverse events identified in the risk assessment profile, meeting risk mitigation requirements. Mitigations will depend on the technologies used and the threats of concern in the risk assessment. For example, systems may have a holdover capability to mitigate temporary service disruptions (see BP.AS.03). Also see the anti-jamming and anti-spoofing mitigation examples in BP.AS.10 and BP.AS.11, respectively.

BP.AS.09 Ensure PNT UE has robust input interfaces with conformance verification..... 16

Input interfaces should include conformance verification checks to monitor incoming signals and ensure valid message contents. Anomalies can indicate data spoofing. PNT signal monitoring may include allow-listing, integrity verification, authentication, or other signal health checks. All incoming data should be checked before it is stored, used, or output. If conformance verification cannot be implemented at the interface, data can be provided to downstream processors for verification. When illegal or invalid message contents are detected, they should be reported and rejected and appropriate backup or holdover sources of PNT information should be used (see BP.AS.03). Suspicious information should also be recognized and reported. Government reference software that implements allow-list checking should be used to guide implementation and to verify operation of anti-data spoofing.

BP.AS.10 Develop PNT UE with anti-jam capabilities 16

PNT UE should be developed with anti-jam capabilities to operate through high received levels of interference and jamming. Techniques to remove unwanted interference or jamming include narrowband excision and signal processing that suppresses constant modulus interference or that estimates and subtracts structured interference or jamming. These techniques can be included in the receiver processing or by adding additional hardware (see BP.AS.06).

BP.AS.11 Develop PNT UE with anti-measurement spoof processing 16

PNT UE should be specified and developed to provide good anti-measurement spoofing—recognizing, rejecting, and reporting spoofing signals that cause the receiver to produce erroneous time of arrival measurements or frequency of arrival measurements. Upon recognition and reporting of spoofing signals, PNT UE should automatically use different sources of PNT information, such as holdover with a precision clock or inertial sensors (see BP.AS.03). Examples of anti-measurement spoofing techniques include:

BP.AS.12 Ensure PNT UE has secure configuration interfaces and appropriate documentation..... 17

PNT UE should include configurability settings and commands that support initialization and resets (see BP.AS.16). Configuration access should be secure (see BP.AS.17 and BP.DO.09). Examples of configuration options include stationary modes, fixed height, or control over included or excluded signals, constellations, or sensors. Manufacturers should provide instructions to calibrate and configure PNT UE appropriately, including when and how to use different settings and features (see BP.DO.01). Consistency of configuration settings, options, and features across devices facilitates streamlined testing and evaluation (see BP.AS.28).

BP.AS.13 Ensure PNT UE has standard output observables and reporting to enable testing and evaluation 18

At output interfaces, PNT equipment should provide an adequate set of well-defined observables and state information to enable test and evaluation (see BP.AS.27), which can also support detection of anomalies and monitoring of situational awareness in larger systems or networks. PNT UE should also report at the output anomalies and threats like jamming and spoofing that are detected internal to the equipment.

BP.AS.14 Enable secure remote access and management for PNT UE 18

When onsite access and management are not possible or sufficient, it should be possible to securely connect PNT UE to a network for management and information extraction.

BP.AS.15 Ensure PNT UE has adverse event recovery capabilities..... 18

PNT systems should support a recovery capability to restore PNT devices to nominal operation and performance after an adverse event. PNT systems may also include automatic recovery capabilities. The UE should allow users to easily upgrade or downgrade firmware or software (see BP.AS.18).

BP.AS.16 Ensure PNT UE has robust reset capabilities 19

PNT UE should have capabilities to undergo robust reset and to clear portions of volatile or non-volatile memory if needed (see BP.AS.29). Remote reset capabilities allowing the user to command reset without physical access to the PNT UE should be secure (see BP.AS.14).

BP.AS.17 Ensure PNT UE incorporates software assurance and cybersecurity 19

All components in PNT devices should have implemented and documented software assurance and cybersecurity practices employed in their design (7). Software should be written so that the processing returns to a known good state either manually by an external command or automatically if the processing is determined to be in an unacceptable state. For example, software should monitor its own operation for situations, such as endless looping, and command a return to a known good state.

BP.AS.18 Plan for software and firmware updates..... 19

Ensure all firmware can be updated and software and firmware updates are routinely issued over secure interfaces. Equipment should have the capability to retain a current software version while downloading a new version that can provide bug fixes, enhancements, and defenses against additional threats. When a new software version is installed, there should be a user-selectable time for switchover to that new version, allowing multiple systems to switch over synchronously. The interface for

upgrading the software should be nonproprietary, with full open or government-owned documentation. Software upgrade processes should rely on strong authentication, and, in many cases, it may be desirable for upgrades to be enabled only by a physical setting on the unit. Even after an update is installed and enabled, PNT UE should be able to return to the previous software version, if necessary.

BP.AS.19 Plan for growth when developing hardware 19

Receiver and processor hardware should be architected and designed for adaptability and growth. Ample margin (perhaps at least 50%) should be left in computing resources and storage to accommodate growth in software functionality and size.

BP.AS.20 Acquire and configure PNT UE to meet use case needs 20

Buy PNT UE that meets the performance and resilience needs of the use case or application, as defined by planning, risk assessment and requirements best practices (see Section 3.1 Best Practices for Organizational Business Processes, Policies, and Procedures). Configure PNT UE appropriately for the operating conditions and environment.

BP.AS.21 Emphasize trust during procurement..... 20

Practice good supply chain hygiene by acquiring equipment from proven and established manufacturers, sources, and service providers when possible.

BP.AS.22 Create test plans for foreseeable adverse PNT events..... 20

Produce plans for qualification and testing to evaluate PNT UE performance during known or foreseeable adverse events (e.g., UTC [Coordinated Universal Time] leap seconds or GPS week number rollovers).

BP.AS.23 Define example PNT UE test suites for reference by manufacturers, evaluators, procurers, and operators..... 20

This should include PNT UE test methods, terminology, and metrics, as well as documentation sufficient for reproducibility.

BP.AS.24 Ensure evidence of testing threat protections are made available to the user .. 21

Ensure evidence of threat testing and protections are made available to the user, including validation of anti-jam and anti-spoof capabilities, as well as foreseeable adverse events (see BP.AS.22).

BP.AS.25 Ensure PNT UE has qualified performance specifications..... 21

In addition to typical performance metrics in nominal conditions, ensure performance metrics are provided for adverse operating conditions, including threat and disruption

situations when one or more external PNT sources may not be available. When using multiple PNT services, ensure that specifications for each clarify performance with and without supplemental sources.

BP.AS.26 Create test equipment for extended PNT use cases..... 21

Use cases vary by PNT source and type of PNT UE. The baseline test equipment covers nominal PNT performance under relevant use cases. Subcategories of the baseline may include (1) varying Position, Velocity, and Time (PVT) sources (e.g., sources from GNSS constellations and other sensors), (2) PNT outputs and dynamics (e.g., PVT vs. timing only, or stationary vs. moving), (3) PNT signal availability, and (4) PNT UE operating modes and initialization. In addition to testing nominal performance, test equipment can enable extended use cases, including:

BP.AS.27 Ensure observables relevant to PNT UE testing are provided over output interfaces 22

Useful observables include PNT signals tracked, inputs used in output formulation (e.g. data messages), QoS metrics such as RF channel power, automatic gain controls, and pseudo-ranges. Signal-to-noise and carrier-to-noise ratios are particularly useful, provided testers use the correct definition and estimation methods (21). See BP.AS.13 for PNT UE design considerations regarding output observables.

BP.AS.28 Seek consistency of and documentation of PNT UE operational modes, settings, and features to support improved testing, automation, and resilience..... 22

Because of differences in applications, requirements, and technology, different types of PNT UE necessarily vary in modes, settings, and features; for example, stationary modes may be appropriate for some timing receivers (see BP.AS.12 and BP.DO.01), while other receivers may include options for fixed height or control over included or excluded sources, such as individual signals, constellations, or sensors. Additional enhancements may include anti-jam and anti-spoof capabilities or automatic gain control (AGC). Users and evaluators should follow manufacturer instructions to determine when to enable or disable certain features and should understand the associated considerations and tradeoffs. Evaluators should document all configuration settings used during testing.

BP.AS.29 Seek consistency of and documentation of resets, programmability, and initialization 22

Document demonstrated PNT UE capabilities to undergo robust reset and to clear portions of volatile or non-volatile memory (see BP.AS.16). Confirm the ability to easily upgrade or downgrade PNT UE firmware or software (see BP.AS.18). Seek standardization of ways to initialize necessary data, modes, and settings to facilitate testing and streamline evaluation procedures.

BP.DO.01 Use appropriate, site-specific, configuration settings and calibrate equipment. 23

Ensure configuration settings consistent with the use case conditions are selected, following manufacturer documentation for the PNT UE (see BP.AS.12). All equipment should be calibrated following manufacturer instructions to compensate for site-specific characteristics.

BP.DO.02 Carefully select antenna locations..... 23

Install PNT signal antennas >10 m away from (and at least slightly above) nearby structures to ensure that the local multipath environment is benign and antenna beam patterns are not distorted. Choose a location where the antenna has an adequate view of the sky. Consider hazards such as birds and lightning/inclement weather in site selection.

BP.DO.03 Obfuscate visibility of the primary antenna 23

Install PNT signal antennas at sites not visible from publicly accessible locations or obscure their exact locations to mitigate tampering, disruption, and deception. When feasible, at an appropriate distance from the primary, add one or more secondary (decoy) antennas connected to a situational awareness sensor.

BP.DO.04 Avoid the reception of low-elevation PNT RF signals where possible 24

Especially when using horizon-nulling PNT antennas (see BP.AS.06), ensure that timing receivers do not use measurements from low-elevation (e.g., < 25°) satellites, since those signals are attenuated by the horizon-nulling antennas. Even if horizon nulling-antennas are not used, consider the benefits of excluding measurements taken at lower elevation angles, since they usually have poorer quality—signals generally received at lower power and more strongly degraded by ground interference and other propagation phenomena.

BP.DO.05 Monitor for outages in PNT infrastructure services..... 24

Because many PNT systems, such as GPS receivers, use infrastructure outside the user's control, document QoS guarantees and dependencies and set up an alert system to remain informed of potential or scheduled outages or degraded services from PNT service providers.

BP.DO.06 Automate detection of adverse PNT events 24

Design data flows to and from PNT equipment to support the detection and reporting of adverse PNT events and conditions. Employ automatic fault detection and alerts, using detection thresholds determined by tests of nominal and anomalous data. When possible, use designs that incorporate multiple PNT sensors, which supports the direct comparison of PNT signals, since disagreements between PNT systems

may indicate adverse events. Monitor the environment according to sensor type and use case.

BP.DO.07 Appropriately manage identities and credentials 24

Enforce use of appropriate identification and authentication credentials for PNT users, PNT applications, and data sources to ensure proper use of resources and integrity of data, and revoke credentials when users no longer need access. Assess the effects of authentication and encryption protocols, because, for example, processing delays can affect PNT services, which often depend on real-time processing.

BP.DO.08 Maintain PNT system software and securely update firmware when needed 24

PNT UE is commonly implemented as software systems with an assortment of interfaces and network connections; therefore, firmware and/or software should be securely updated throughout the product lifecycle.

BP.DO.09 Practice good cyber hygiene 25

Follow good cyber hygiene practices, since both the GPS receiver and any associated processors are computers (often networked). Install and maintain firewalls, virus protection, and other defenses, such as protections applied to any other mission-critical computing system. Authenticate software patches and updates and then apply them promptly. Require two-factor authentication, including strong passwords, for access. Change all factory default and maintenance passwords and update them regularly. If continuous network connectivity is unnecessary, it may be prudent to operate without a network connection except when such a connection is needed.

BP.DO.10 Assess PNT UE operational performance..... 25

Maintain logs of operational PNT UE performance. Operators and maintainers serve as the front line for evaluating the compliance of PNT UE serving CI and provide key inputs to update and improve organizational policies and procedures regarding PNT.

BP.DO.11 Keep PNT UE audit logs in compliance with regulations and legal requirements 25

Maintain audit logs, using existing standard data formats where possible and including identities of individuals and components that may be affected by adverse events. PNT applications with an audit trail sometimes require legal or metrological traceability (22; 23; 24; 25; 26).

BP.D0.12 Report suspicious PNT UE events and adverse conditions to appropriate authorities..... 25

The public and private sectors operate systems that collect information on the availability and performance of widely adopted PNT UE. These data are invaluable in identifying and responding to service outages.