FEDERAL POSITIONING, NAVIGATION, AND TIMING (PNT) SERVICES ACQUISITIONS GUIDANCE (Version 1.0)

Publication: February 2024
Cybersecurity and Infrastructure Security Agency

Table of Contents

Table of Figures

Table of Tables

ACKNOWLEDGEMENTS

Stakeholders from both industry and government provided significant input and collaboration to facilitate development of this guidance. The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) acknowledges and thanks all those who contributed to this guidance.

The following people/organizations contributed to the development of Version 1.0 of this guidance.

NAME	AFFILIATION
Ken Alexander	Aviation Safety, Federal Aviation Administration, U.S. Department of Transportation
Brandon Beers	National Coordination Office for Space-Based PNT, U.S. Department of Transportation
Kelsey Blaskoski	Office of the Under Secretary of Defense for Acquisition and Sustainment, U.S. Department of Defense
Robert Bridenstine	Coast Guard Acquisition Directorate, U.S. Coast Guard
Barry Bruno	Alaskan Satellite Telecommunications Infrastructure, Federal Aviation Administration, U.S. Department of Transportation
Andrew Christen	System Protection and Control Systems, Bonneville Power Administration
Jeff Dagle	Pacific Northwest National Laboratory
Tobias Erickson	Western Area Power Administration
Kevin Funk	Office of Governmentwide Acquisition Policy, U.S. General Services Administration
Louis Gallegos	Federal Aviation Administration, U.S. Department of Transportation
Daniel Hamai	Western Area Power Administration
Lannie Herlihy	Federal Aviation Administration, U.S. Department of Transportation
Dave Howard	Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy
Carrol Larvick	Western Area Power Administration
Tracey Lawrence	Maritime Administration, U.S. Department of Transportation
Steve Mackey	Volpe National Transportation Systems Center, U.S. Department of Transportation
George Mantis	Volpe National Transportation Systems Center, U.S. Department of Transportation
Aaron Martin	Western Area Power Administration

NAME	AFFILIATION
Harold “Stormy” Martin	National Coordination Office for Space-Based PNT, U.S. Department of Transportation
Michael Pelkey	Under Secretary of Defense for Acquisition and Sustainment, U.S. Department of Defense
James Platt	Positioning, Navigation, and Timing, National Risk Management Center, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security
Nancy Pomerleau	Stakeholder Engagement Division, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security
Noah Rosen	Federal Aviation Administration, U.S. Department of Transportation
Michael Roskind	Positioning, Navigation, and Timing, National Risk Management Center, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security
Paul Shaw	Cybersecurity, Technical Subject Matter Expert, Defense Acquisition University, U.S. Department of Defense
Michael Striffolino	Positioning, Navigation, and Timing, National Risk Management Center, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security
Karen VanDyke	Office of the Assistant Secretary for Research and Technology, U.S. Department of Transportation
Hadi Wassaf	Volpe National Transportation Systems Center, U.S. Department of Transportation
Ernest Wong	Science and Technology Directorate, U.S. Department of Homeland Security

DISCLAIMER

This guidance is voluntary and does not: constitute regulations, define mandatory practices, provide a checklist for compliance, or carry statutory authority. It is intended to be a set of guidelines.

BACKGROUND

The Cybersecurity and Infrastructure Security Agency (CISA), in concert with the Federal Positioning, Navigation, and Timing (PNT) Contract Language Development Working Group, developed the *Federal PNT Services Acquisitions Guidance*[1] to streamline and support the implementation of PNT model contractual language as instructed by Presidential Executive Order 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services (EO 13905)*. This effort is in support of DHS's requirement under EO 13905. CISA led the coordination and collaboration for this "living" guidance to incorporate interagency and cross-sector acquisition recommendations for PNT resiliency requirements.

Per EO 13905, section 4, subsection (d), the guidance provides workflows, steps, and recommended structures, "…for requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services." The Federal PNT Contract Language Development Working Group carried out actions and product development as instructed through EO 13905, section 4, subsections (c), (d), and (e):

> (c) Within 1 year of the date of this order, the Secretary of Homeland Security, in coordination with the heads of Sector-Specific Agencies (SSAs), shall develop a plan to test the vulnerabilities of critical infrastructure systems, networks, and assets in the event of disruption and manipulation of PNT services. The results of the tests carried out under that plan shall be used to inform updates to the PNT profiles identified in subsection (a) of this section.
>
> (d) Within 90 days of the PNT profiles being made available, the heads of SSAs and the heads of other executive departments and agencies, as appropriate, through the Secretary of Homeland Security, shall develop contractual language for inclusion of the relevant information from the PNT profiles in the requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services. The heads of SSAs and the heads of other agencies, as appropriate, shall update the requirements as necessary.
>
> (e) Within 180 days of the completion of any of the duties described in subsection (d) of this section, and consistent with applicable law and to the maximum extent practicable, the Federal Acquisition Regulatory Council, in consultation with the heads of SSAs and the heads of other agencies, as appropriate, shall incorporate the requirements developed under subsection (d) of this section into Federal contracts for products, systems, and services that integrate or use PNT services.

This guidance offers an overarching view of the model contractual language construction process to aid PNT program managers, acquisition professionals, and contract bidders in assessing their PNT dependencies. It also establishes requirements for appropriate levels of resiliency based upon the operational needs of the proposed product, system, or service.

The National Institute of Standards and Technology's (NIST) Internal Report 8323, Revision 1 NIST.IR.8323r1, explains that, "…PNT data is generated by cyber systems. Protection of the devices and systems used to generate PNT data should be considered part of cybersecurity." Cybersecurity professionals, engineers, and acquisition professionals for mission critical systems are strongly encouraged to consider protection of devices and systems used to generate or consume PNT data as part of a system's cybersecurity posture.

There are several national documents that inform federal acquisitions personnel's need to assess and evaluate the use of Global Navigation Satellite Systems (GNSS), including the Global Positioning System (GPS) and foreign GNSS systems within their system of systems designs and acquisitions as directed in EO 13905.

- *Federal Communications Commission (FCC) Order 18-158, Waiver of Part 25 Licensing Requirements for Receive-Only Earth Stations Operating with the Galileo Radionavigation-Satellite Service* states, "…we grant the requested waivers for non-Federal receiver operations with two of the Galileo signals, E1 and E5…"

[1] Hereafter referred to as the "guidance."

- *National Space Policy (NSP)* (December 9, 2020) states, "Promote the responsible use of United States space-based PNT services and capabilities in civil and commercial sectors at the Federal, State, and local levels, including the utilization of multiple and diverse complementary PNT systems or approaches for national critical functions."
- *Space Policy Directive 7 (SPD-7)* (January 15, 2021) states, "Use of multiple, varied PNT services can result in better performance in terms of user accuracy, availability, and resilience. However, the United States Government does not assure the reliability or authenticity of foreign PNT services."

Individual departments should avoid using other foreign constellations for the determination of PNT since these constellations may present undocumented vulnerabilities with no method of mitigation.

REVIEW THE GUIDANCE WORKFLOW

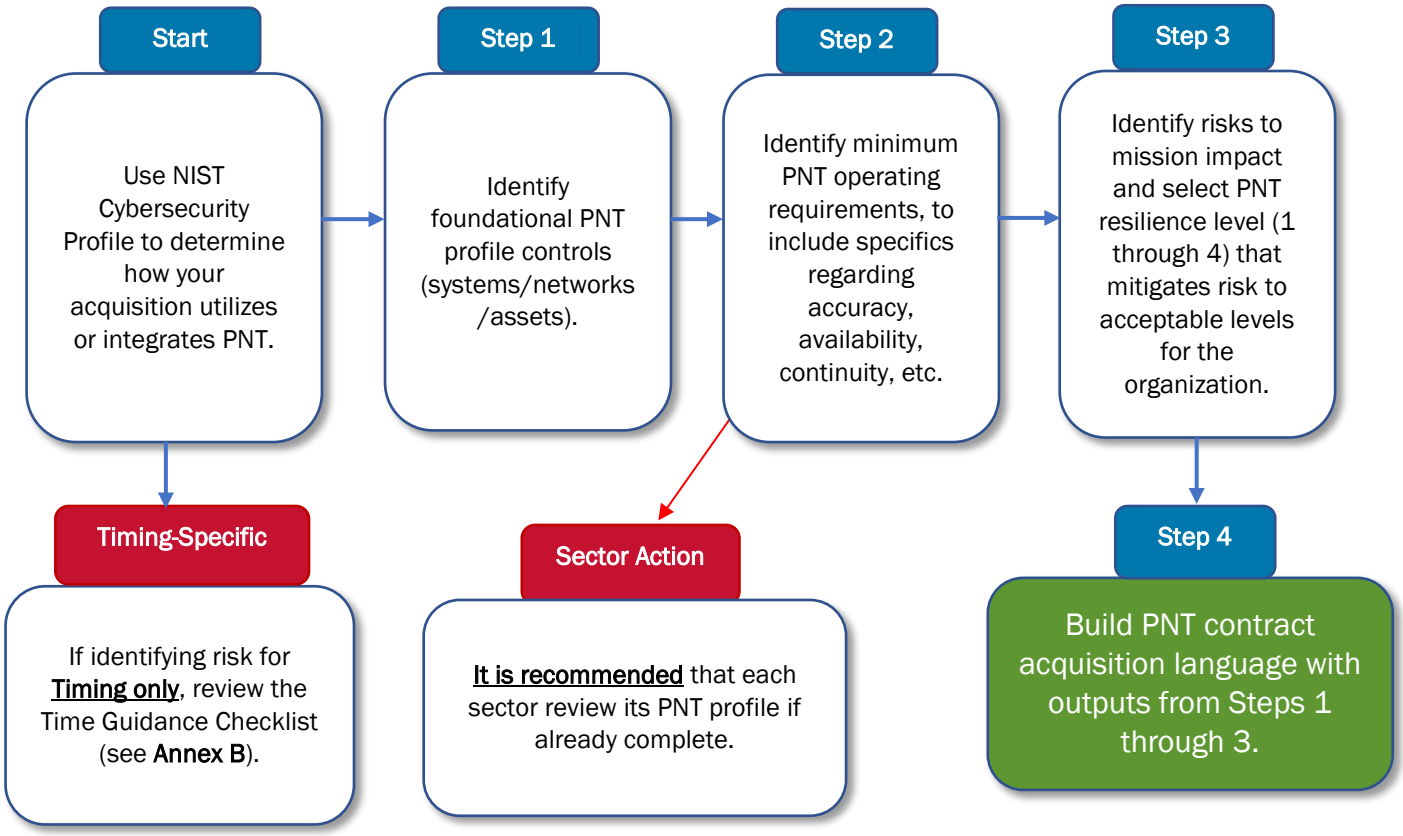


FIGURE 1 – GUIDANCE WORKFLOW

START – DETERMINE IF CONTRACT/ACQUISITION INVOLVES USE OF PNT

To begin, consider how the U.S. Department of Transportation (DOT) and NIST define PNT and whether those definitions reflect the services, products, or systems related to your acquisition. Determining that your acquisition uses PNT suggests that this guidance is the next (and best) step for your acquisition. If unsure about PNT use, assume your acquisition uses PNT until you confirm there is no use of PNT by going through the PNT Cybersecurity Profile. Note that most communications and information technology systems are heavily dependent upon timing services, and other critical infrastructure is often dependent upon positioning, navigation, and/or timing data.

DOT explains that PNT is a combination of three distinct, constituent capabilities:

- **Positioning**, the ability to accurately and precisely determine one's location and orientation two-dimensionally (or three-dimensionally when required) referenced to a standard geodetic system (such as World Geodetic System 1984, or WGS84).
- **Navigation**, the ability to determine current and desired position (relative or absolute) and apply corrections to course, orientation, and speed to attain a desired position anywhere around the world, from sub-surface to surface and from surface to space.
- **Timing**, the ability to acquire and maintain accurate and precise time from a standard (Coordinated Universal Time), anywhere in the world and within user-defined timeliness parameters. Timing also includes time transfer. Many find timing services their most significant risk to operations of the three capabilities and may only be interested in addressing and mitigating *timing only* as part of a procurement.

Furthermore, EO 13905 describes PNT services 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."

When PNT is used in combination with satellites and other information (e.g., weather or traffic data) to form a navigation system with global coverage, the result is called a Global Navigation Satellite System (GNSS), with the most recognizable service example being the Global Positioning System (GPS). While PNT encompasses so much more than navigational functions, GPS is a major component.

Question: Do any definitions/examples relate to your PNT product, system, or services? **Proceed to Step 1 – Identify Foundational PNT Profile Controls.** Go through the Foundational PNT Profile Controls to make an informed decision and, if needed, consult a PNT expert.

Question: Did you find that only the **Timing** definition was relevant to your PNT product, system, or services? **Skip to Step 2 – Identify Minimum Operating Requirements for use of PNT data** and review **Annex B – Time Guidance Checklist**.

STEP 1 – IDENTIFY FOUNDATIONAL PNT PROFILE CONTROLS

Review the prioritized PNT subcategories of NIST.IR.8323r1 and descriptions below to identify foundational PNT profile controls—the most important risk and mitigation attributes for your PNT acquisition (systems, networks, and assets). Additional and specific mitigation measures are outlined in the NIST.IR.8323r1. Mark the controls you need to protect your PNT services. If your sector-specific PNT Profile is complete or near completion, the Federal PNT Contract Language Development Working Group recommends reviewing it ahead of completing this step.

TABLE 1 – PRIORITIZED NIST.IR.8323R1 SUBCATEGORIES

Function	Subcategory	Description	NIST.IR.8323r1 Page #
Identify	Asset Management-3	Organizational communication and data flows are mapped.	Page 16
	Asset Management-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	Page 18

Function	Subcategory	Description	NIST.IR.8323r1 Page #
	Business Environment-4	Dependencies and critical functions for the delivery of critical services are established.	Page 20
	Business Environment-5	Resilience requirements to support the delivery of critical services are established for all operating states (e.g., under duress or attack, during recovery, normal operations).	Page 21
	Governance-4	Governance and risk management processes address cybersecurity risks.	Page 22
	Risk Assessment-1	Asset vulnerabilities are identified and documented.	Page 24
	Risk Assessment-3	Threats, both internal and external, are identified and documented.	Page 26
	Risk Assessment-4	Potential business impacts and likelihoods are identified.	Page 27
	Risk Assessment-5	Threats, vulnerabilities, likelihoods, and impacts are used to assess risk.	Page 28
	Supply Chain Risk Management-2	Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	Page 30
Protect	Access Control-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	Page 33
	Access Control-2	Physical access to assets is managed and protected.	Page 33
	Access Control-3	Remote access is managed.	Page 34
	Access Control-4	Access permissions and authorizations are managed, incorporating the	Page 34

Function	Subcategory	Description	NIST.IR.8323r1 Page #
		principles of least privilege and separation of duties.	
	Access Control-5	Network integrity is protected (e.g., network segregation, network segmentation).	Page 34
	Access Control-6	Identities are proofed and bound to credentials and asserted in interactions.	Page 35
	Access Control-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	Page 35
	Data Security-4	Adequate capacity to ensure availability is maintained.	Page 39
	Data Security-6	Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	Page 40
	Data Security-8	Integrity checking mechanisms are used to verify hardware integrity.	Page 42
	Information Protection-3	Configuration change control processes are in place.	Page 44
	Protective Technology-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	Page 51
	Protective Technology-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	Page 52
Detect	Anomalies and Events-3	Event data are collected and correlated from multiple sources and sensors.	Page 54

Function	Subcategory	Description	NIST.IR.8323r1 Page #
	Security Continuous Monitoring-1	The network is monitored to detect potential cybersecurity events.	Page 56
	Security Continuous Monitoring-4	Malicious code is detected.	Page 58
	Security Continuous Monitoring-6	External service provider activity is monitored to detect potential cybersecurity events.	Page 58
Respond	Analysis-5	Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).	Page 68
	Mitigation-3	Newly identified vulnerabilities are mitigated or documented as accepted risks.	Page 70
	Improvements-2	Response strategies are updated.	Page 71
Recover	Improvements-2	Recovery strategies are updated.	Page 74

Once finished, you should have a curated table of subcategories like the example below. **The sample selections below are for demonstration purposes ONLY.**

TABLE 2 – SAMPLE SELECTED NIST.IR.8323R1 SUBCATEGORIES

Subcategory	Description	NIST.IR.8323r1 Page #
RA-1	Asset vulnerabilities are identified and documented.	Page 24
AC-2	Physical access to assets is managed and protected.	Page 33
CM-4	Malicious code is detected.	Page 58
AN-5	Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).	Page 68

Subcategory	Description	NIST.IR.8323r1 Page #
RP-1	Recovery plan is executed during or after a cybersecurity incident.	Page 73

RISK AND VULNERABILITY USE CASE ENVIRONMENT

PNT is an essential utility for many critical operations. Disruption of or interference to PNT services can have adverse, cascading impacts on individuals, businesses, and the nation's economic and national security.

Risk identification is the process of identifying and defining potential risks that could impact—deny, manipulate, or otherwise compromise—successful transmission of positioning, navigation, or timing signals. Review the table below to assist in identifying risks and associated vulnerabilities as well as determining the most appropriate risk mitigation strategies for your product, system, or services that use and may be critically dependent upon PNT data.

NIST defines risk mitigation as prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Well documented risks to the PNT mission include the following in Table 3, and at a minimum, should be evaluated as potential risks for your PNT acquisition. You should also consider sector-specific PNT risks. Additional DHS recommendations may be found at Improving the Operation and Development of GPS Equipment Used by Critical Infrastructure.

TABLE 3 – UNDERSTANDING PNT RISKS AND VULNERABILITIES

PNT-Related Threat	Vulnerability	Recommended Mitigation(s)	Real-World Examples[2]
Signal Jamming When a malicious actor sends a powerful radio signal to interfere with the GPS signal, causing it to be lost or distorted	• Disrupting transportation • Interfering with military operations • Cyberattacks	• Spectrum monitoring and detection tools (e.g., anomalous PNT inputs) • Anti-jamming technologies (e.g., front-end level [Automatic Gain Control (AGC)] and pre-correlation level [multi-constellation multi-frequency (MCMF)], and Controlled Radiation Pattern Antennas [CRPA]) • Adopt multiple PNT sources (redundancy) • Practice good cyber hygiene • Employ high quality holdover devices	Denver, CO (January 2022) Dallas-Fort Worth (October 2022)
Signal Spoofing (Measurements and Data) When a malicious actor sends false PNT signals to a receiver, tricking it into thinking it is in a different location	• Disrupt communication and navigation systems • Potential accidents and threats to public safety • Cyberattacks	• Sensor fusion • Obscure antenna • Decoy antenna • Redundant antenna • Spatial filtering • Adopt multiple PNT sources (redundancy) • Practice good cyber hygiene	GPS Spoofing – Black Sea (June 2017)

[2] All examples use open-source information.

Outputs for Step 1 include:

- Your curated table of selected NIST.IR.8323r1 subcategory controls (mitigation)
- All identified risks, vulnerabilities, and mitigations based on your PNT acquisition use cases
- Any other sector-specific operational requirements or conditions

STEP 2 – IDENTIFY MINIMUM OPERATING REQUIREMENTS FOR USE OF PNT DATA

After selecting the appropriate PNT NIST.IR.8323r1 subcategories in the previous step, identify the minimum operating requirements for your product, system, or services that use PNT data, to include specifics regarding PNT accuracy, availability, continuity, and integrity (error bounding).

PNT OPERATIONAL REQUIREMENTS

The August 2018 Government Accountability Office Report to Congressional Requesters titled *DHS Acquisitions: Additional Practices Could Help Components Better Develop Operational Requirements* describes operational requirements as, "…what the end users need to fill capability gaps and conduct the mission. Operational requirements, in part, define the purpose for the acquisition program and set boundaries for user needs. Subject matter experts, such as system engineers, support development of operational requirements to ensure that they are clearly developed. Well-defined operational requirements trace to one or more of the identified capability gaps."[3]

The Department of Energy, Office of Electricity, highlights EO 13905 key definitions in its *Response to NIST Request for Information (RFI) about Profile of Responsible Use of PNT Services* that are critical in grasping and further defining your PNT operational boundaries and parameters:

> **PNT Profile**: A description of the responsible use of PNT services—aligned to standards, guidelines, and sector-specific requirements—selected for a particular system to address the potential disruption or manipulation of PNT services.
>
> **PNT Services**: 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.
>
> **Responsible Use of PNT**: The deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government.

Essential elements of PNT, likely present in most systems, include accuracy, availability, continuity, and integrity of signals. PNT operational requirements and information technology and operational technology (IT/OT) configurations **vary widely by sector,** and those requirements change over time. Reviewing your sector's PNT profile informs minimum PNT operational requirements for your acquisition as you consider the essential PNT elements mentioned above. An example of how the essential PNT elements, specific definitions, and parameters can be represented in acquisition language are depicted in the section below. At the highest level, this example defines the overall PNT system needs guided by elements of EO 13905 and Department of Defense (DoD) acquisitions requirements (for model purposes).

[3] U.S. Government Accountability Office, Report to Congressional Requesters, "DHS Acquisitions: Additional Practices Could Help Components Better Develop Operational Requirements," August 2018, https://www.gao.gov/assets/700/693951.pdf. Accessed on August 30, 2023.

*The [insert sector/department/agency] requires a PNT [insert product, system, or service] that integrates and/or utilizes PNT Services. The PNT Service is integrated with or utilizes a [insert system, network, or capability] that provides a reference to [calculate or augment the calculation of] [insert **accuracy and integrity** parameters of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof].*

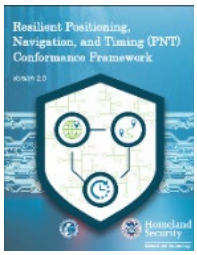
*Overall, the system or service must be hardened to withstand [insert **availability and continuity** parameters] and recover from jamming or spoofing incidents and not subject to single point, common cause dependent failure.*

*The PNT system or service shall have the ability to **detect** an anomaly with 100% **recoverability** from the anomaly (e.g., jamming or spoofing) within [provide time parameter and to what level of a degraded state], and have a trusted PNT solution after a denial, manipulation, or degradation of GPS service at full operational state within [insert time parameter].*

Output for Step 2 includes:

- Your minimum PNT operational requirements (informed by engineering or sector-specific PNT profile and subject matter expertise)

STEP 3 – SELECT MOST APPROPRIATE PNT RESILIENCE LEVEL



After identifying the minimum operating requirements in Step 2, Step 3 involves selecting resilience level requirements that mitigate risk to acceptable levels for the organization. DHS's Science and Technology Directorate (S&T) Resilient PNT Conformance Framework provides general guidance for assessing requirements and resilience levels that stakeholders may consider for PNT product, system, or service operational needs. CISA included this framework for reference and conceptual grounding while the Institute of Electrical and Electronics Engineers' (IEEE) P1952 *Resilient PNT User Equipment Working Group* develops a standard for resilient PNT user equipment (at the time of this publication, standards development is in progress).

RESILIENT CONFORMANCE FRAMEWORK MINIMUM REQUIREMENTS FOR RESILIENCE LEVELS

Once you establish the minimum operational requirements for use of PNT data in Step 2, start with those requirements in mind as you review the Conformance Framework's Minimum Requirements for PNT Resilience Levels below:

LEVEL 1 – ENSURES RECOVERABILITY AFTER REMOVAL OF THE THREAT

- Must verify that stored data from external inputs adhere to values and formats of established standards.
- Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat.
- Must include the ability to securely reload or update firmware.

LEVEL 2[4] – PROVIDES A SOLUTION (POSSIBLY WITH UNBOUNDED[5] DEGRADATION) DURING THREAT

Includes capabilities enumerated in Level 1 plus:

[4] Critical infrastructure applications will likely require Level 2 resilience at a minimum.
[5] The output can deviate within a manufacturer-defined envelope.

- Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions.
- Must support automatic recovery of individual PNT sources and system, without disrupting system PNT output. Positioning, navigation, or timing can be critical to the functions that the system, product, or service provides (e.g., cell phones and laptop computers).

LEVEL 3 – PROVIDES A SOLUTION (WITH BOUNDED DEGRADATION) DURING THREAT

Includes capabilities enumerated in Levels 1 and 2 plus:

- Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source.
- Must cross-verify between PNT solutions from all PNT sources.

LEVEL 4 – PROVIDES A SOLUTION WITHOUT DEGRADATION DURING THREAT

Includes capabilities enumerated in Levels 1, 2, and 3 plus:

- Must have diversity of PNT source technology to mitigate common mode threats.[6]

Considering compiled information on PNT subcategory controls, identified risks, threats, vulnerabilities, and mitigations for your PNT acquisition, select a **PNT resilience level (1 through 4)** in accordance with your analyses.

Output for Step 3 includes:

- A selected PNT resilience level (1 through 4) for your PNT acquisition

Proceed to **Step 4.**

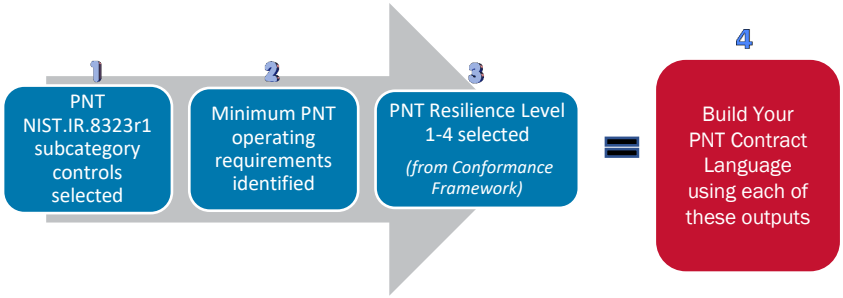
STEP 4 – BUILD PNT CONTRACT LANGUAGE WITH OUTPUTS FROM STEPS 1-3

Step 4 is the building or compilation step in putting together PNT contract language for your acquisition. Take a moment to review your outputs from Steps 1 through 3, building the content as you go. Annex A of this document details how the Federal Aviation Administration (FAA) approached the drafting and implementation of PNT acquisition/contract language for internal acquisition life cycle management.

Note: CISA initiated the PNT contract language development effort as a first step to serve as a baseline for future efforts. Sector-specific profiles are not yet complete. As companies and organizations create these profiles and their own templates, the Federal PNT Contract Language Development Working Group will provide exemplars as annexes to this living guidance. In the interim, please refer to the guidance for interagency and cross-sector informed recommended PNT language construction.

[6] U.S. Department of Homeland Security. Science and Technology Directorate. "Resilient Positioning, Navigation, and Timing Conformance Framework version 2.0." May 31, 2022. https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework.

In accordance with this ***Federal PNT Services Acquisitions Guidance***, use the selected subcategories from **Step 1**, the minimum operating requirements from **Step 2,** and the PNT resilience level from **Step 3** to inform your choices. Fill in the recommended format below to build the appropriate contract wording/structure for your PNT acquisition, contract, or services.



KEY PNT REFERENCE DOCUMENTS

These key PNT reference documents include external supporting information, best practices, and standards. The Federal PNT Contract Language Development Working Group will update the reference document set as relevant and informing guidance becomes available. All documents can be found at https://www.cisa.gov/federal-pnt-services-acquisitions-contract-language.

- Executive Order 13905 - Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services
- DHS Science and Technology Directorate's "Resilient PNT Conformance Framework" (2.0)
- NIST Technical Note 2187 "A Resilient Architecture for the Realization and Distribution of Coordinated Universal Time to Critical Infrastructure Systems in the United States"
- NIST Technical Note 2189 "An Evaluation of Dependencies of Critical Infrastructure Timing Systems on the Global Positioning System (GPS)"
- NIST.IR.8323r1 "Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services."
- Federal Information Security Modernization Act (FISMA) of 2014 (amends FISMA 2002)
- IEEE 1588 – 2008 – "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems"
- Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure
- Time Guidance for Network Operators, Chief Information Officers, and Chief Information Security Officers
- NIST SP-800-18 (Rev. 1) - Guide for Developing Security Plans for Federal Information Systems
- FAA Timing Order 1770.68 – Selection and Use of Time and Frequency Sources for all Systems, Services, and Applications Supporting NAS Operations
- The National Space Policy

- FCC Order 18-158, Waiver of Part 25 Licensing Requirements for Receive-Only Earth Stations Operating with the Galileo Radionavigation-Satellite Service
- Space Policy Directive 7 (SPD-7)
- FAR DFARS Operating Guide (2015)

ANNEX A – PNT PROCUREMENT LANGUAGE DEVELOPMENT EXAMPLES

Annex A details how the Federal Aviation Administration (FAA) approached the drafting and implementation of PNT acquisition/contract language for internal acquisition life cycle management. The FAA use case serves as a regulatory exemplar of the PNT procurement language development process, implementation, and execution.

The FAA initiated a data call across the National Airspace System (NAS) of over 150 system-of-systems, assessing NAS GPS use and dependence. The FAA follows its own Acquisition Management System (AMS) for policy and guidance for all aspects of lifecycle acquisition management. In November 2020, the FAA issued *Timing Order 1770.68 – Selection and Use of Time and Frequency Sources for all Systems, Services, and Applications Supporting NAS Operations*, of which section 4(b)(1) requires the following:

> (1) …Therefore, the FAA will develop and incorporate the "contractual language for inclusion of the relevant information from the [positioning, navigation, and timing (PNT)] profiles in the requirements for [FAA] contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services" into the FAA's Acquisition Management System approximately 90 days following the PNT profiles being made available by Secretary of Commerce.

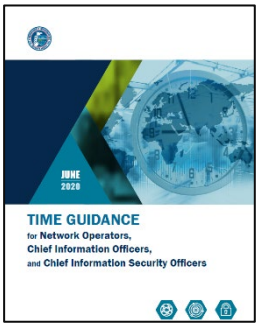
The FAA explained that they are developing a waiver process for the Timing Order, as well as a bench test and accompanying best practices.

The resulting AMS Procurement Guidance (Contract Language - April 2022) became effective April 2022 and states:

> (g) Positioning, Navigation, and Timing (PNT) Services. "PNT services" means 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. In accordance with FAA Order 1770.68 (Selection and Use of Time and Frequency Sources for all Systems, Services, and Applications Supporting NAS Operations), PNT requirements must be included in all solicitations, contracts, and orders for products, systems, and services that integrate or utilize Time and Frequency (T&F) systems or services. The Office of Primary Responsibility (OPR) for PNT requirements is the NAS Enterprise Analysis Branch (ANG-B21). The requiring service organization must contact ANG-B21 to determine PNT applicability.

ANNEX B – TIME GUIDANCE CHECKLIST

IMPORTANT: If you are identifying risk for timing focused PNT products', systems', or services' operational requirements, the Federal PNT Contract Language Development Working Group recommends that you review this checklist.



The Time Guidance for Network Operators, Chief Information Officers, and Chief Information Security Officers offers a comprehensive DHS-vetted resource of best practices for timing requirements. Accurate PNT is necessary for the functioning of many critical infrastructure sectors. Precision timing is particularly important and is primarily provided through the GPS. However, GPS's space-based signals are low-power and unencrypted, making them susceptible to both intentional and unintentional disruption.

1. Know Your Systems
   a. Managing timing and synchronization devices used in your network and all connections through contracted data communications services.

Testing Questions:

- ☐ Do you have policies governing the distribution of time of day and or frequency on your network?
- ☐ Can you identify which servers provide time across your network? Do you have traceability from time servers to Stratum 1 clocks? Do those servers acquire time from a Stratum 1 time reference?
- ☐ If a GPS or GNSS receiver is providing time on your network, are you including the receiver in your standard IT inventory and providing regular software/firmware updates per manufacturer recommendations? *SPD-7*, states, "…Use of multiple, varied PNT services can result in better performance in terms of user accuracy, availability, and resilience. However, the United States Government does not assure the reliability or authenticity of foreign PNT services…"
- ☐ Do you scan your network regularly for time servers?

   b. Identify the applications or systems that require time for operation within your organization.

Testing Questions:

- ☐ Have you validated that these products, systems, or services use time and/or frequency?
- ☐ What level of accuracy, with respect to UTC (NIST)/UTC (USNO), are the systems reliant on time and/or frequency need?
- ☐ Do you have a time source and distribution method that meets the level of accuracy identified in the testing question above?

   c. Maintain an inventory of your organization's time-dependent systems.

Testing Questions:

- ☐ Does your organization have an inventory of time-dependent systems and their precision requirements?
- ☐ Does your organization have an inventory of timing and synchronization devices?
- ☐ Does your organization have a means of keeping this inventory current?
- ☐ Is time-reliance documented in your system architecture?

   d. Is your system capable of detecting time anomalies?

Testing Questions:

- ☐ Do you have a published level of service for timing?
- ☐ Do you have a way to identify or monitor the level of service (if defined)?

- Are you able to notify your users if your network is not performing to the published level of service agreement?
- Is your system capable of detecting anomalies? For example, if your time jumps backward or forward.

e. Do you know how long your system and critical applications can maintain nominal operation in the absence of synchronization to a primary time source?

Testing Questions:

- Has your organization identified a holdover time for each time-reliant system and application in your inventory?
- Has the holdover time been approved by end users (have you validated that it meets business or mission requirements)?
- Has regular preventative maintenance been performed to ensure holdover devices are operationally ready and maintain quality if the reference source degrades?

f. Do you understand how the system reacts when time accuracy is degraded?

Testing Questions:

- Are systems designed to inform critical, time-dependent applications that timing is degraded and may not be reliable?
- Do applications have error handling routines to address degraded or unreliable time?
- Are operators trained to respond to GPS receiver alarms/fault indications?
- Do you have an alternate/backup source of timing to go to should your primary time source be degraded?

2. Know Your Timing Source(s)

a. Managing timing and synchronization devices used in your network.

Testing Questions:

- What is your primary source of time?
- Do you have a secondary time source identified and configured?
- What level of accuracy (i.e., seconds, milliseconds, or microseconds) is provided by your time source?
- Does that source meet your requirements for time?
- Are processes defined to resolve time source discrepancies?

b. Do you have a regulatory level of service requirement for your system or application? Determine the level of time performance needed for your system or application.

Testing Questions:

- Can your systems tolerate degradation to level of service?
- Are your systems able to holdover for *x* hours/days until external time returns?
- Are your systems able to operate without your time source for any length of time? For example, does the system have a holdover capability (internal oscillator) that enables some level of service during a disruption of primary source(s)?

c. Are all GPS receivers in compliance with the latest GPS Interface Control Document (ICD)? The latest version of the GPS ICD can be found on the GPS ICD page.

Testing Questions:

- Have you checked for firmware updates to comply with ICD updates?

d. Do you have an authentication scheme to verify your time comes from a legitimate time server(s)?

Testing Questions:

- Have you tested time servers and validated authenticity?

3. Know Your Users
   a. Do your users have regulatory requirements for time on their system or application? Is this captured in your service-level agreement?
   b. Do you know whether your customers depend on your systems/network as a source of accurate time?
   c. Have you published a level of service for timing on your network?
4. Regularly Update Your System
   a. Practice good cyber hygiene within your network as well as with special-purpose time equipment. Regularly update your systems and firmware, being sure to validate the integrity of any firmware or software by confirming the code is signed or that checksums provided match.

Testing Questions:

- Do you deploy firewalls and use virus protection?
- Are software patches and system updates installed once available?
- Updates are located at the NTP Downloads page. The network manager should maintain a file or log of NTP software/firmware versions of each client.
- The NTP Security Notice site can provide vulnerability and mitigation details and is located at the NTP Security Notice Page.
- Are timing and synchronization devices routinely patched?
- Do you receive push notifications from vendors when patches are available?
- Are GPS timing receivers installed in accordance with DHS best practices?

   b. When incorporating new timing sources or devices, consider full lifecycle cybersecurity with best practices built-in at the time of product delivery.

Testing Questions:

- Are timing and synchronization devices included in your lifecycle management plan?
- If timing and synchronization devices are not upgradeable, are they scheduled for replacement?
- Does the timing and synchronization equipment have strong default security settings?
- Is the timing and synchronization device and its software/firmware adaptable and upgradeable?

   c. Follow guidance provided by the manufacturer for maintenance and updates to hardware and software to ensure optimal operation of your equipment.
   d. Regularly back up data and files (i.e., configuration files, settings, etc.).
5. Document and Test Your System and Sources
   a. Have processes in place to validate your internal and external time source(s).

Testing Questions:

- For timing systems and devices, have you documented processes for maintenance, testing, and validation?

- Do you have time maintenance, time anomaly, and time recovery procedures documented?
- Are these processes incorporated into your standard operating procedures (SOPs)?
- Are employees familiar and trained on timing systems, device maintenance, and testing protocols?
- Do you perform good cyber hygiene?

b. Test your time equipment to ensure it operates according to your accuracy and precision requirements.

Testing Questions:

- Do you have clear timing protocol policies?
- What time servers are master clock, and how do these clocks acquire their time?
- Are GPS/GNSS timing devices (receivers and antennas) installed and maintained in accordance with DHS best practices?
- Do you have a documented process to establish time after an outage?
- Have you blocked all non-authenticated ports at the firewall for network perimeter security? This includes:

c. Incorporate battery tests and replacement schedules as part of your maintenance schedule. Use an uninterruptable power source (UPS) and test regularly.

d. Using a test bed can be helpful prior to deployment of new or updated systems, but keep in mind there is no guarantee the test bed will operate like the actual network.

e. Test time intervals annually and before and after a known time event (e.g., leap second, Daylight Saving Time).

6. Diversify Your Timing Sources

a. Diversify receiver types (models and manufacturers) within your network; this provides resilience within your network.

b. Use multiple available timing sources (network-based, system clocks, two-way time transfer, etc.) to avoid single points of failure.

c. Understand the benefits, limitations, and risks associated with each timing source.

7. Detect and Address Anomalies in Your Timing Sources

a. Have a way to detect anomalies in your time source(s).

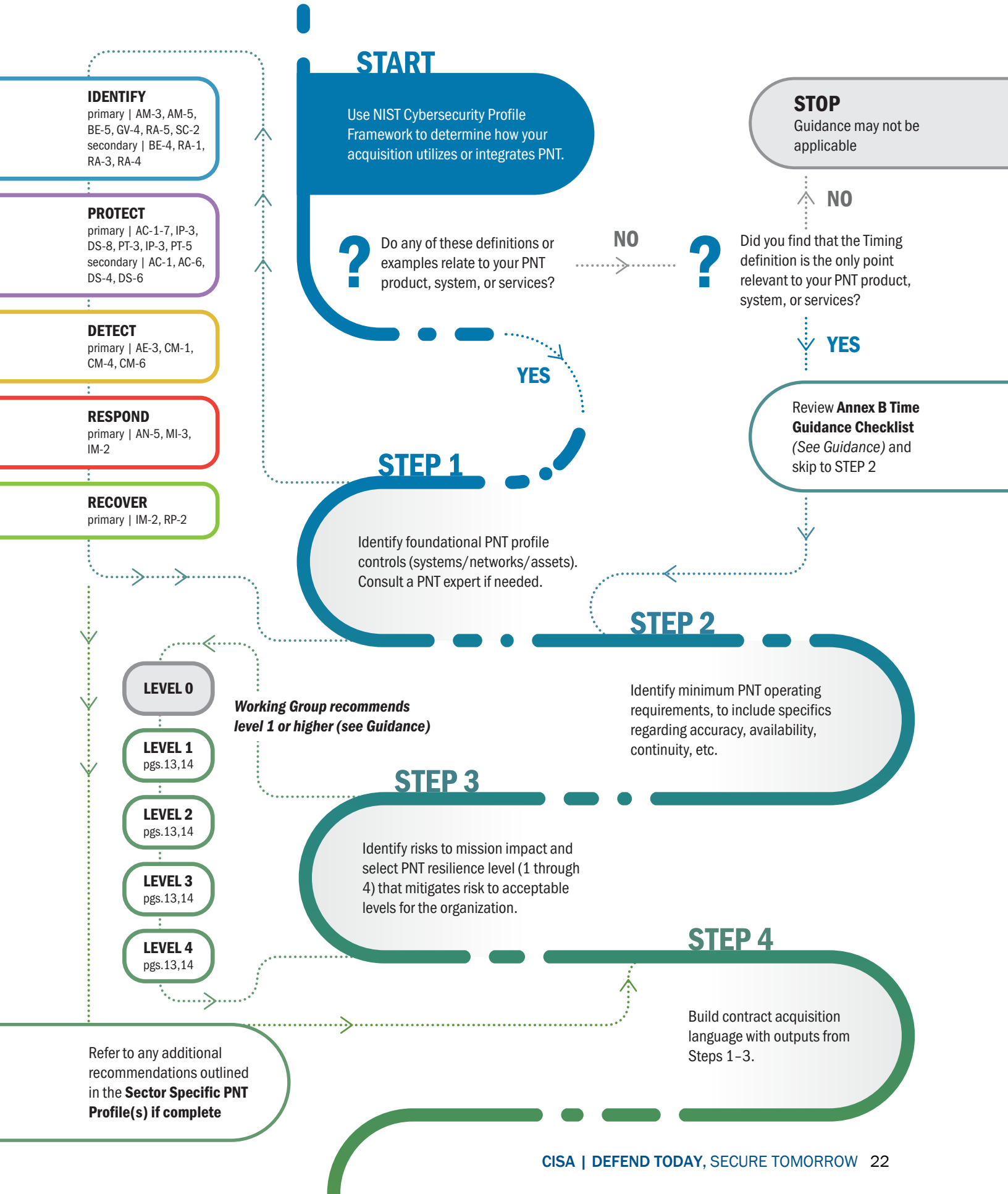
Testing Questions:

- Do you have documented processes to follow should anomalies be detected? These may include audit logs, alerts, etc.
- Are operators/network staff/technical staff trained to respond to alarms that indicate timing issues?

b. Based on your time requirements, do you have equipment, processes, and procedures in place to handle extended time source outages and anomalies?

c. If your primary time source becomes corrupted or unavailable, do you have a process for moving to an alternative time source? Is this external or internal?

ANNEX C – FEDERAL PNT SERVICES ACQUISITIONS GUIDANCE WORKFLOW



PRODUCT SURVEY

The Cybersecurity and Infrastructure Security Agency's National Risk Management Center welcomes your feedback. Please complete the following product survey at https://forms.office.com/g/ajOhrdceFZ, or scan the QR code.