Federal Positioning, Navigation, and Timing (PNT) Services Acquisitions Quick Reference Guide

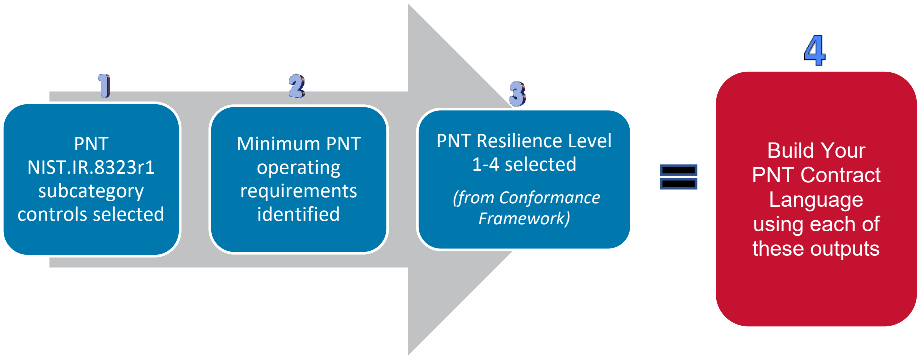
BACKGROUND AND PURPOSE

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 the Department of Homeland Security'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. 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.

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

In accordance with the ***Federal PNT Services Acquisitions Guidance*** at https://www.cisa.gov/resources-tools/resources/federal-positioning-navigation-and-timing-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.



1 PNT NIST.IR.8323r1 subcategory controls selected

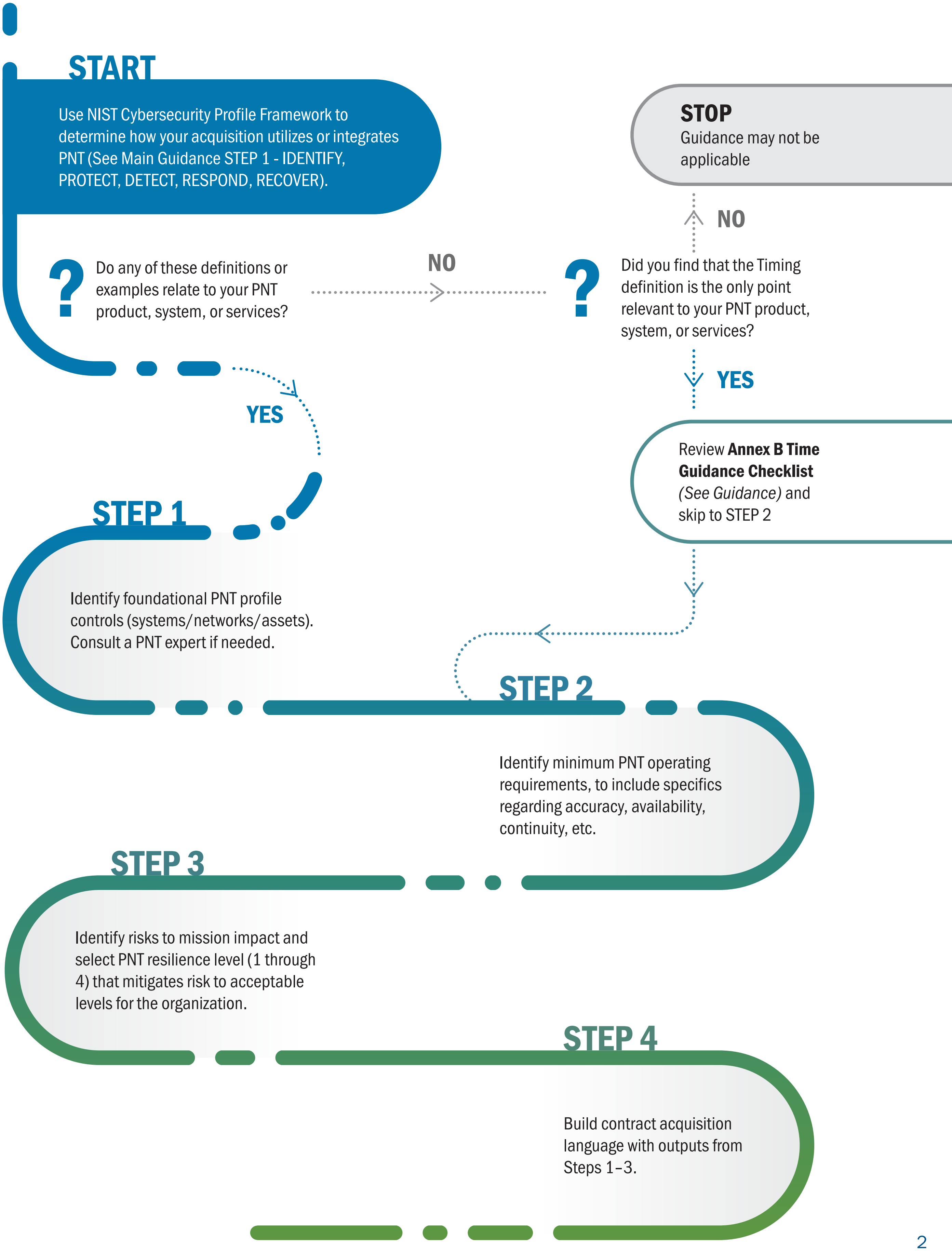
2 Minimum PNT operating requirements identified

3 PNT Resilience Level 1-4 selected *(from Conformance Framework)*

=

4 Build Your PNT Contract Language using each of these outputs

[1] Hereafter referred to as the “guidance.”



START

Use NIST Cybersecurity Profile Framework to determine how your acquisition utilizes or integrates PNT (See Main Guidance STEP 1 - IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER).

? Do any of these definitions or examples relate to your PNT product, system, or services?

NO

? Did you find that the Timing definition is the only point relevant to your PNT product, system, or services?

NO

STOP
Guidance may not be applicable

YES

Review **Annex B Time Guidance Checklist** *(See Guidance)* and skip to STEP 2

YES

STEP 1

Identify foundational PNT profile controls (systems/networks/assets). Consult a PNT expert if needed.

STEP 2

Identify minimum PNT operating requirements, to include specifics regarding accuracy, availability, continuity, etc.

STEP 3

Identify risks to mission impact and select PNT resilience level (1 through 4) that mitigates risk to acceptable levels for the organization.

STEP 4

Build contract acquisition language with outputs from Steps 1–3.