POSITIONING NAVIGATION AND TIMING

CGSIC
September 2024

National Risk Management Center

CISA NRMC PNT RESILIENCE

EO-13905 Contract Language for Federal Acquisitions (Implementation Section 4d)

A. *Developed Guidance for Risk Based Federal contract language for PNT resilience in coordination with the Interagency and Acquisition Community – Published May 2024*

Federal PNT Services Acquisitions Guidance | CISA

B. PNT Services Acquisitions Guidance is moving forward for incorporation through the FAR Council through DHS Office of the Chief Procurement Officers to become a requirement (FAR Part placement is pending)

C. CISA is developing training videos and technical assistance for use of the Guidance

D. The Guidance is also meant to be used as a voluntary tool by state, local, tribal and industry partners

As a resource please visit:
www.cisa.gov/pnt

and

www.gps.gov

U.S. Department of Homeland Security | Science and Technology Directorate

Resilient Positioning, Navigation, and Timing Research and Development Update

Science and Technology

Michael Wilbur
Program/Project Manager
Mission and Capability Support
Critical Infrastructure Security & Resilience Research (CISRR) Program

Resilient PNT Reference Architecture Implementation

BLUF: Demonstrate how Conformance Framework concepts can reduce risk and lower barriers to commercial development of resilient PNT systems and support Standards Development through the utilization and transition of Reference Architecture concepts.

Objective: Build and demonstrate an implementation of the resilient PNT reference architecture based on prior Conformance Framework and Reference Architecture documents to further build on the Rapid Resilience Evaluation Toolkit.

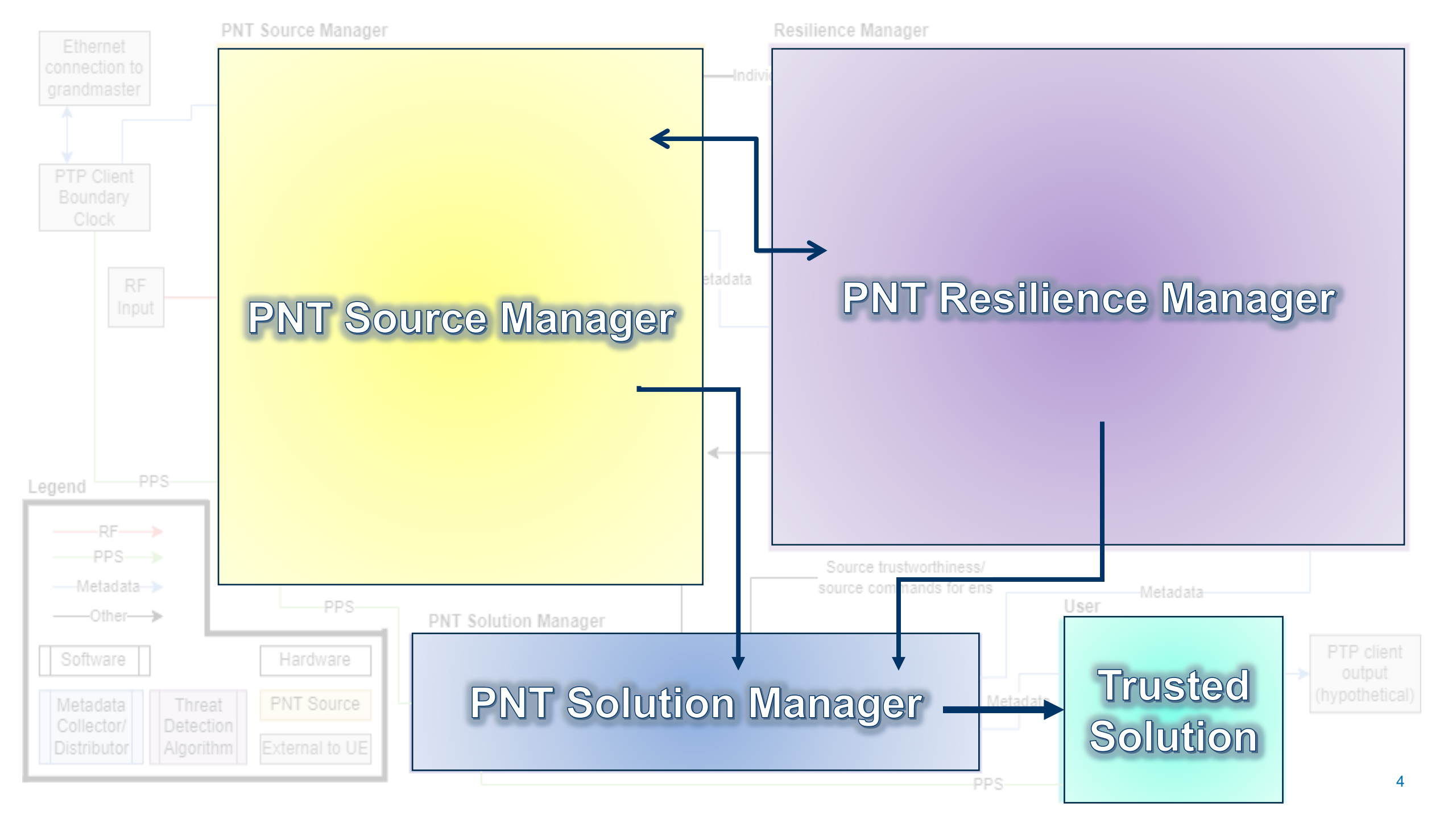
Impact: Demonstrate the feasibility of the resilient PNT reference architecture, which provides a holistic cybersecurity-based approach for Next Generation Resilient PNT user equipment.

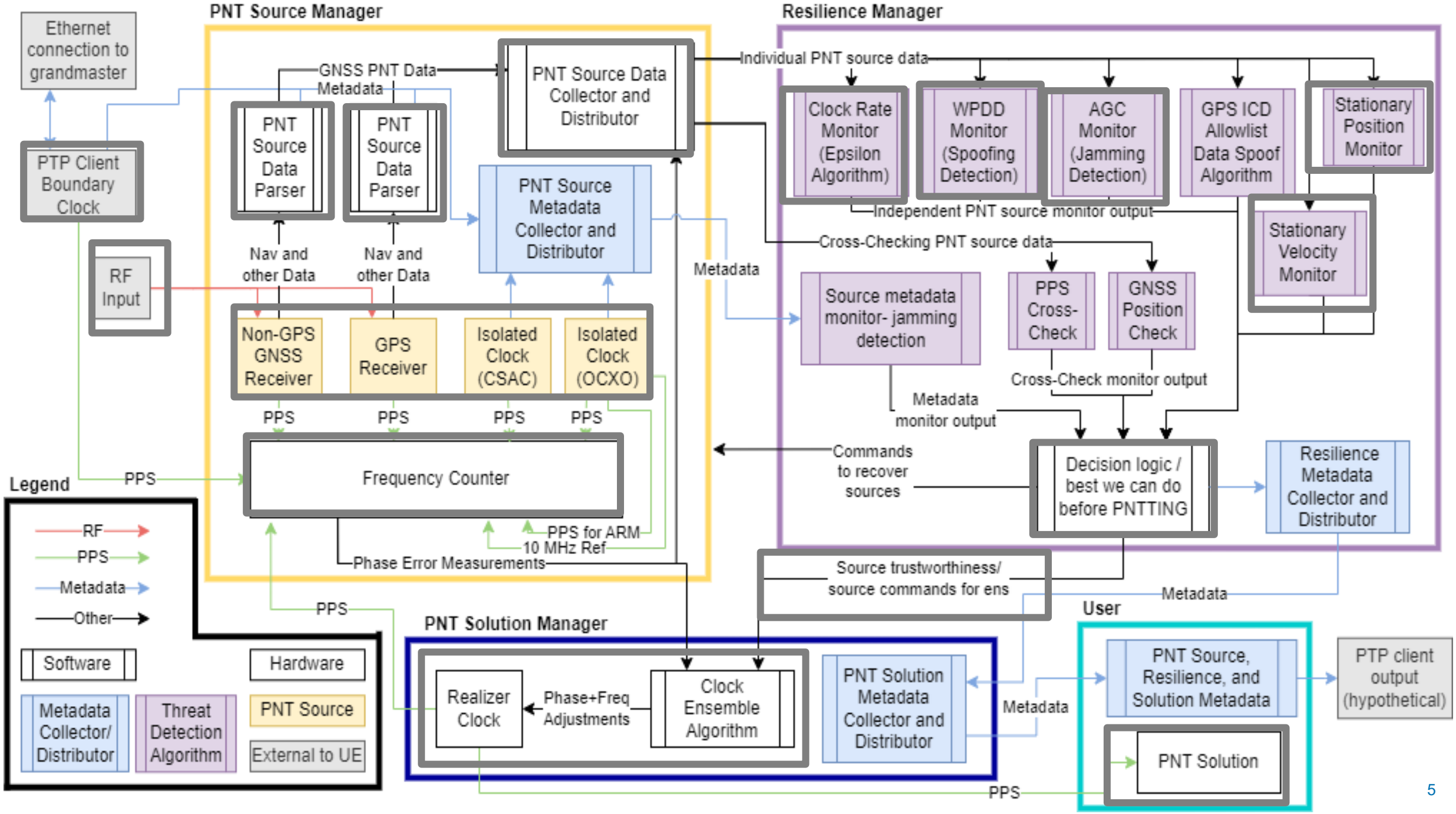
Reference Implementation Design Readiness Review	
Completed	May 2023

Reference Implementation Design Description Document	
Complete	May 2024

Reference Implementation Demonstration Plan	
Complete	November 2023

Reference Implementation Conference Presentation	
Complete	9/16/24


PNT Source Manager
PNT Resilience Manager
PNT Solution Manager
Trusted Solution


PNT Source Manager
Resilience Manager
Ethernet connection to grandmaster
PTP Client Boundary Clock
RF Input
GNSS PNT Data Metadata
PNT Source Data Collector and Distributor
PNT Source Data Parser
PNT Source Data Parser
PNT Source Metadata Collector and Distributor
Nav and other Data
Nav and other Data
Non-GPS GNSS Receiver
GPS Receiver
Isolated Clock (CSAC)
Isolated Clock (OCXO)
PPS
PPS
PPS
PPS
Frequency Counter
PPS for ARM
10 MHz Ref
Phase Error Measurements
Metadata
Individual PNT source data
Clock Rate Monitor (Epsilon Algorithm)
WPDD Monitor (Spoofing Detection)
AGC Monitor (Jamming Detection)
GPS ICD Allowlist Data Spoof Algorithm
Stationary Position Monitor
Stationary Velocity Monitor
Independent PNT source monitor output
Cross-Checking PNT source data
Source metadata monitor- jamming detection
PPS Cross-Check
GNSS Position Check
Cross-Check monitor output
Metadata monitor output
Commands to recover sources
Decision logic / best we can do before PNTTING
Resilience Metadata Collector and Distributor
Source trustworthiness/ source commands for ens
Metadata
User
PNT Source, Resilience, and Solution Metadata
PNT Solution
PTP client output (hypothetical)
PPS
PNT Solution Manager
Realizer Clock
Phase+Freq Adjustments
Clock Ensemble Algorithm
PNT Solution Metadata Collector and Distributor
Metadata
PPS
Legend
RF
PPS
Metadata
Other
Software
Hardware
Metadata Collector/ Distributor
Threat Detection Algorithm
PNT Source
External to UE

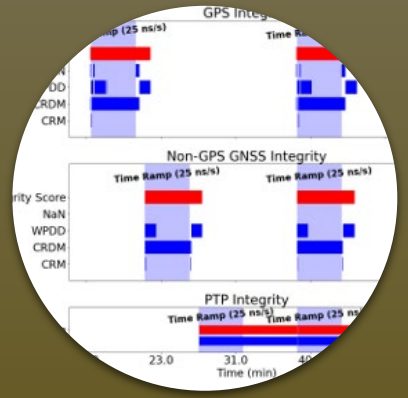
Resilient PNT Reference Implementation (RPNT RI)

- Demonstrates practical applications of the RPNT resilience concepts from the Reference Architecture to reduce vendor risk in producing RPNT User Equipment (UE) for use in Critical Infrastructure.
- The RI Comprises
  - A variety of PNT sources (COTS GNSS) not steered to any external time-base
  - Software to handle the real-time receipt and passing of messages to and from PNT sources
  - Threat monitoring algorithms
  - A monitor fusion engine to combine the outputs of those algorithms to aid in making decisions on the trustworthiness of the PNT sources
  - A timing ensemble with steering to an oscillator to generate a timing 1 Pulse per Second (1PPS) output using trusted sources.
- The RI Expands on previous Rapid Resiliency Evaluation Testbed work that S&T conducted.

Future Efforts (FY25 and beyond…)

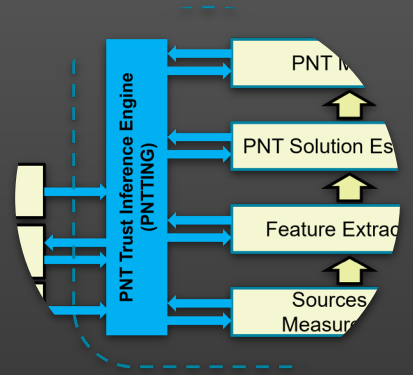
Equipment Testing Framework

- Test Framework development, evaluating resilient PNT system(s)



Analysis and Visualization Tools

- Live visualization of integrity and PVT states



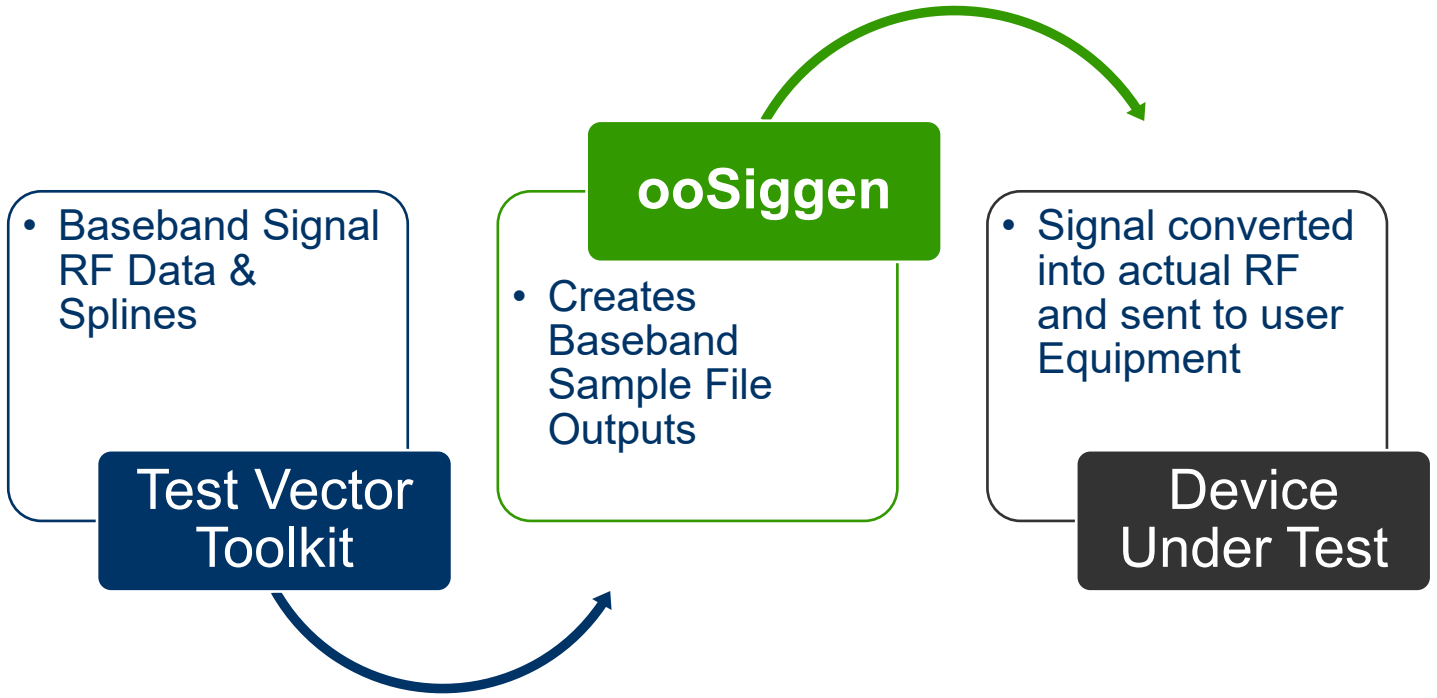
Advanced Monitors

GNSS Test Vector Suite & Distribution Methodology

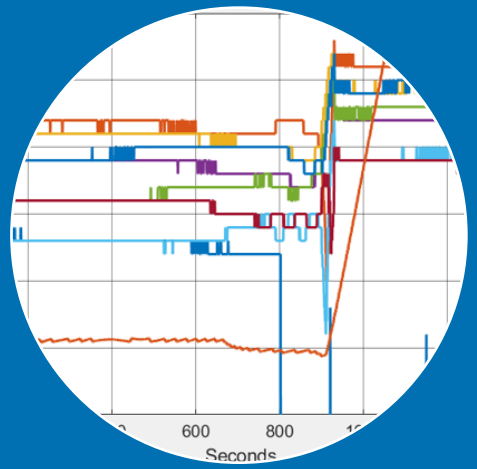
BLUF: This activity has identified and defined appropriate test scenarios that support standards conformity assessment and GNSS Test Vectors based on these test scenarios providing these Test Vectors as a proof-of-concept for distribution to CI end-users.

Objective: GNSS Test Vector Suite & Distribution Methodology: Develop GNSS test vectors to be used for assessing GNSS user equipment resilience and enhance distribution methodologies.

Impact: Enables industry a common set of vectors to use for assessing resilience of GNSS user equipment. This will also help advance conformity assessment work associated with the Institute of Electrical and Electronics Engineers (IEEE) P1952 resilient standards for PNT user equipment.



Science and Technology

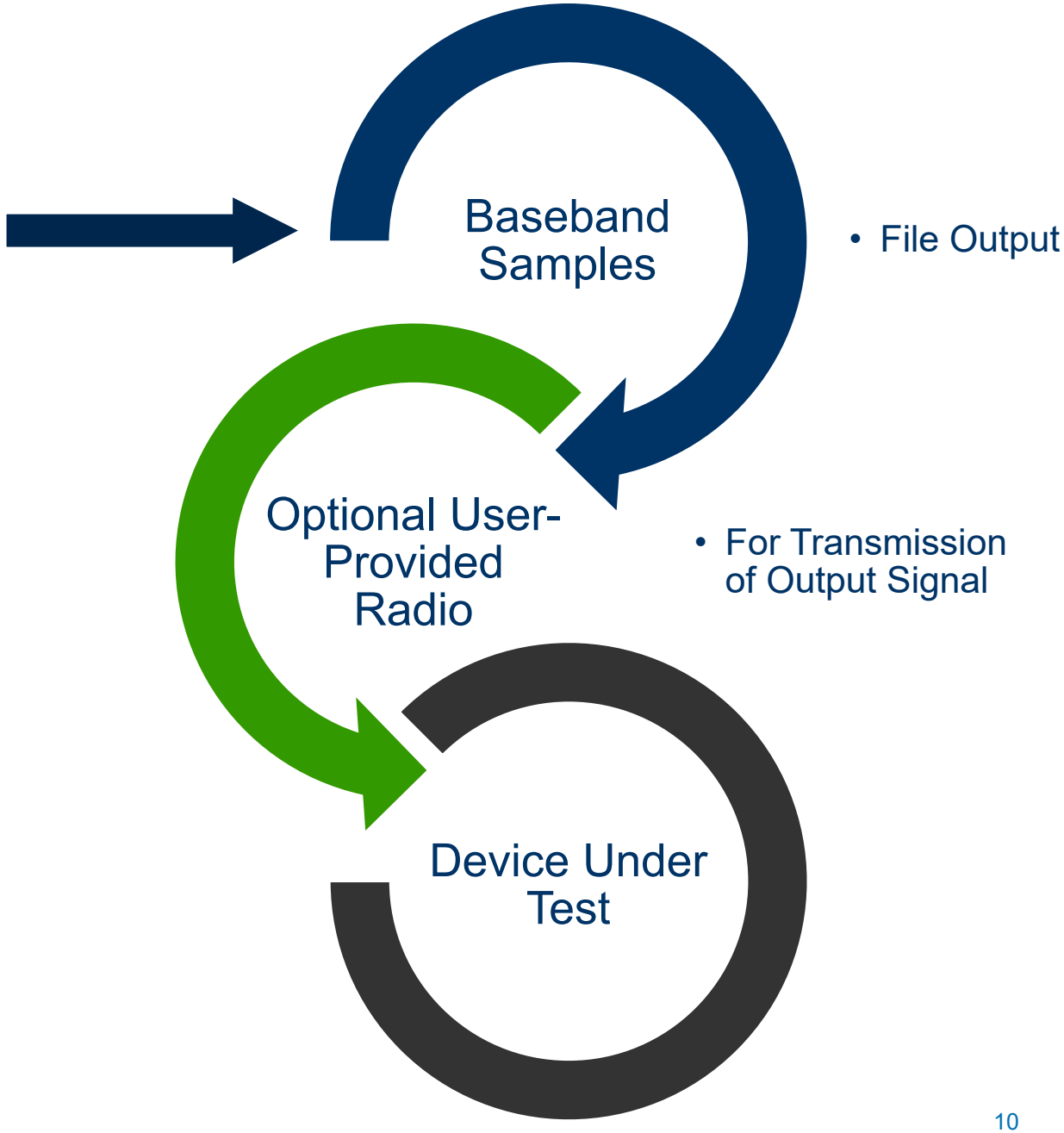


Test Vector (JSON + Splines)

- **JSON File:** *Defines the signals that are present in the test vector and various constant parameters for each signal (center frequency, PRN, etc.)*
- **Splines:** *Parameters that may change over time (E.G. Signal power, Pseudorange, Doppler Shift, Data symbols (supports BPSK and QPSK), Noise power, etc.)*

MITRE Object Oriented Signal Generation Environment (ooSiggen)

- Generates RF much slower than real time (16 hr PC for 10 min of sim on laptop ca 2020) for GPS L1 only including all signals
- Requires one or several relatively low-cost software defined radios for playback
- Creates Baseband Sample File Outputs based on defined parameters

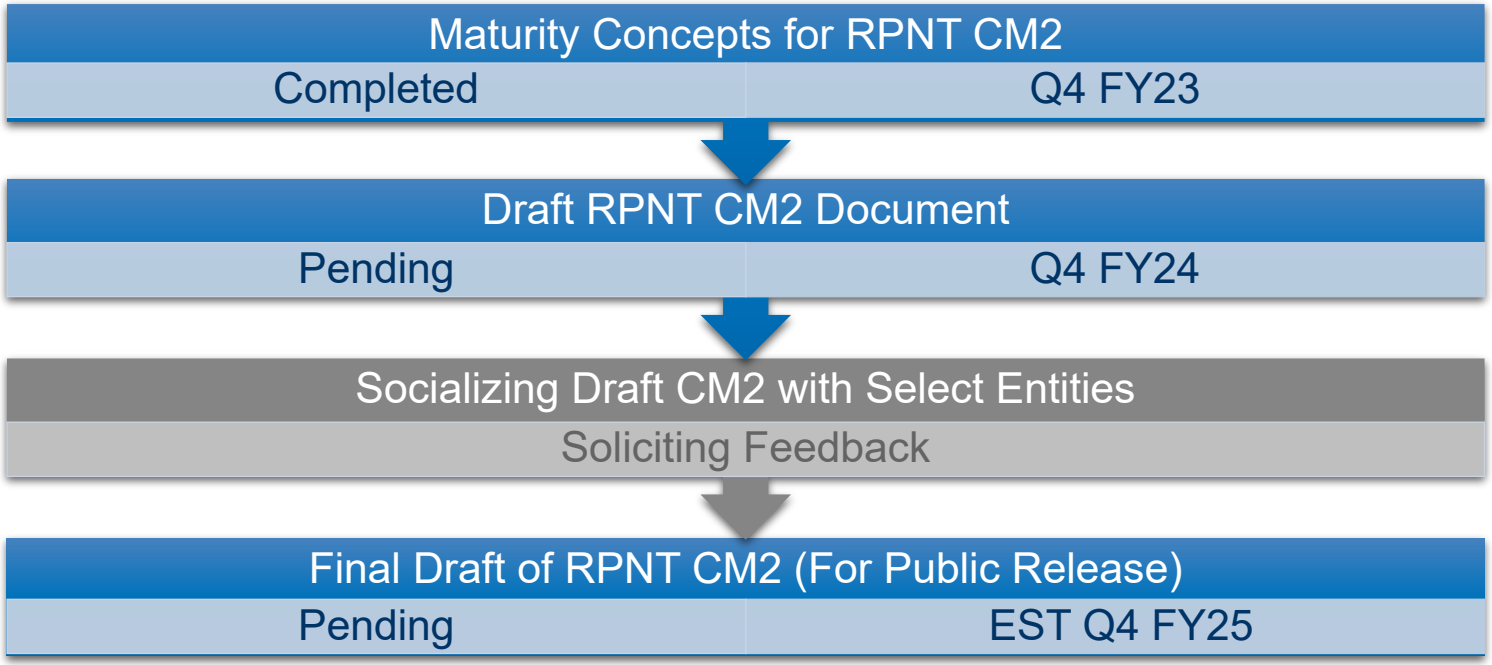


Resilient PNT Capability Maturity Model (RPNT CM2)

BLUF: This Resilient PNT Capability Maturity Model (CM2) establishes a maturity framework and an assessment method and tool, allowing organizations to easily apply recommended PNT profile outcomes and other resilience guidance in an iterative and systematic manner. Through CM2, organizations can assess maturity, identify gaps, and develop action plans and roadmaps to achieve security and resilience aligned to their specific operating environment and vulnerabilities.

Objective: Develop a capability maturity model for organizations to benchmark their PNT resilience and facilitate behaviors, practices, and processes to mature their PNT resilience capabilities. This should build on the NIST Foundational PNT Profile developed in response to Executive Order 13905

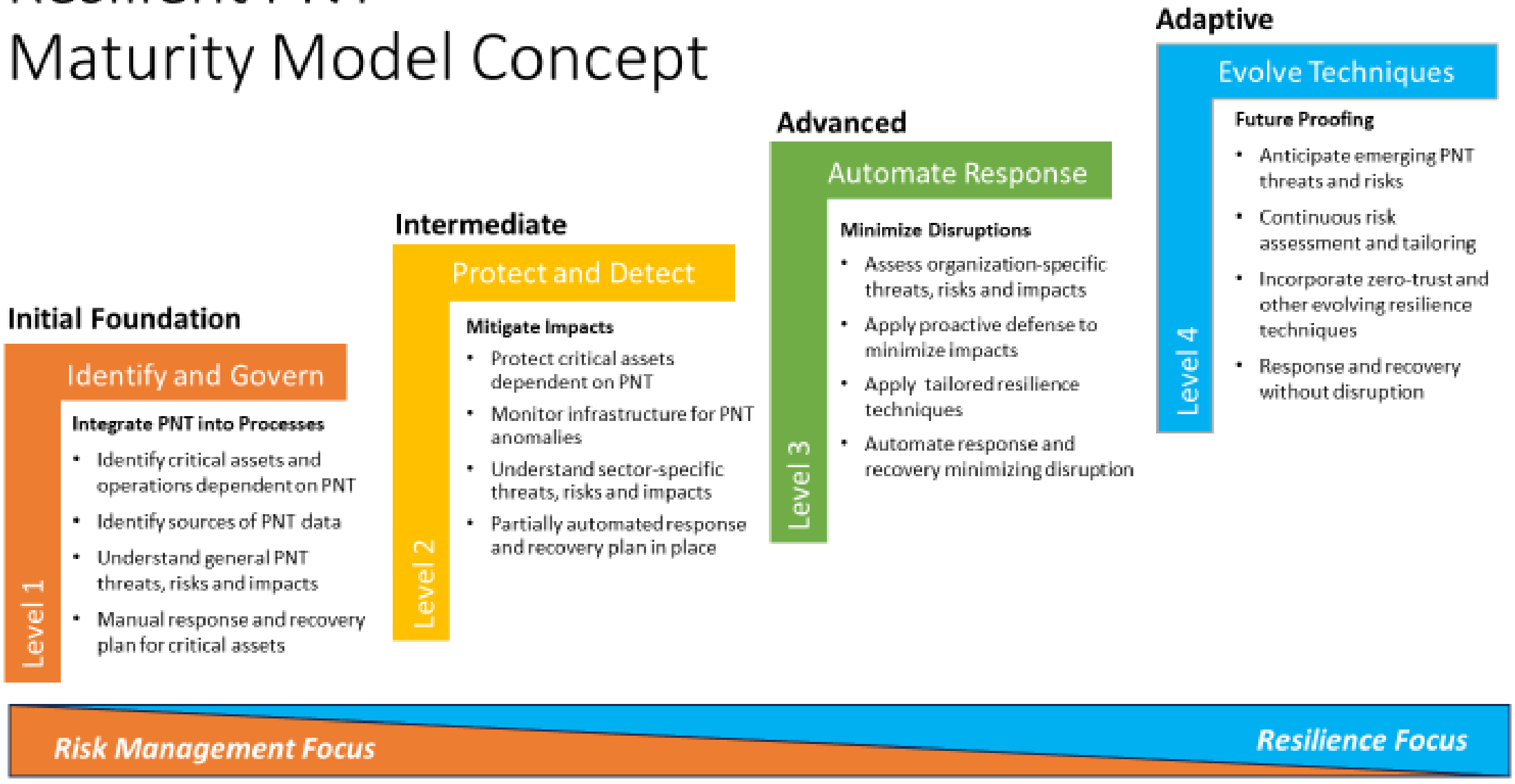
Impact: Enable organizations to understand their resilience to PNT disruptions and how to mature related processes and capabilities.



Capability Maturity Model (CM2) at a Glance

- The CM2 and its assessment tool are designed to support responsible use of PNT through assessment of organizational, operational, and system dependencies on PNT services, infrastructure, and data and integrate related cybersecurity and resilience considerations into their risk management and system acquisition lifecycle and decision-making process.
- The tool is intended for use at various levels and by different roles within an organization.
- The model serves as a maturity benchmark for organizations to identify gaps and build a profile for a more resilient future state.

Resilient PNT Maturity Model Concept



Positioning, Navigation, & Timing Best Practices Guide

Objective: The guide aims to provide CI Owners and Operators, PNT developers, supply chain stakeholders, and service providers with tailorable best practices for development, integration, and use of PNT systems and services.

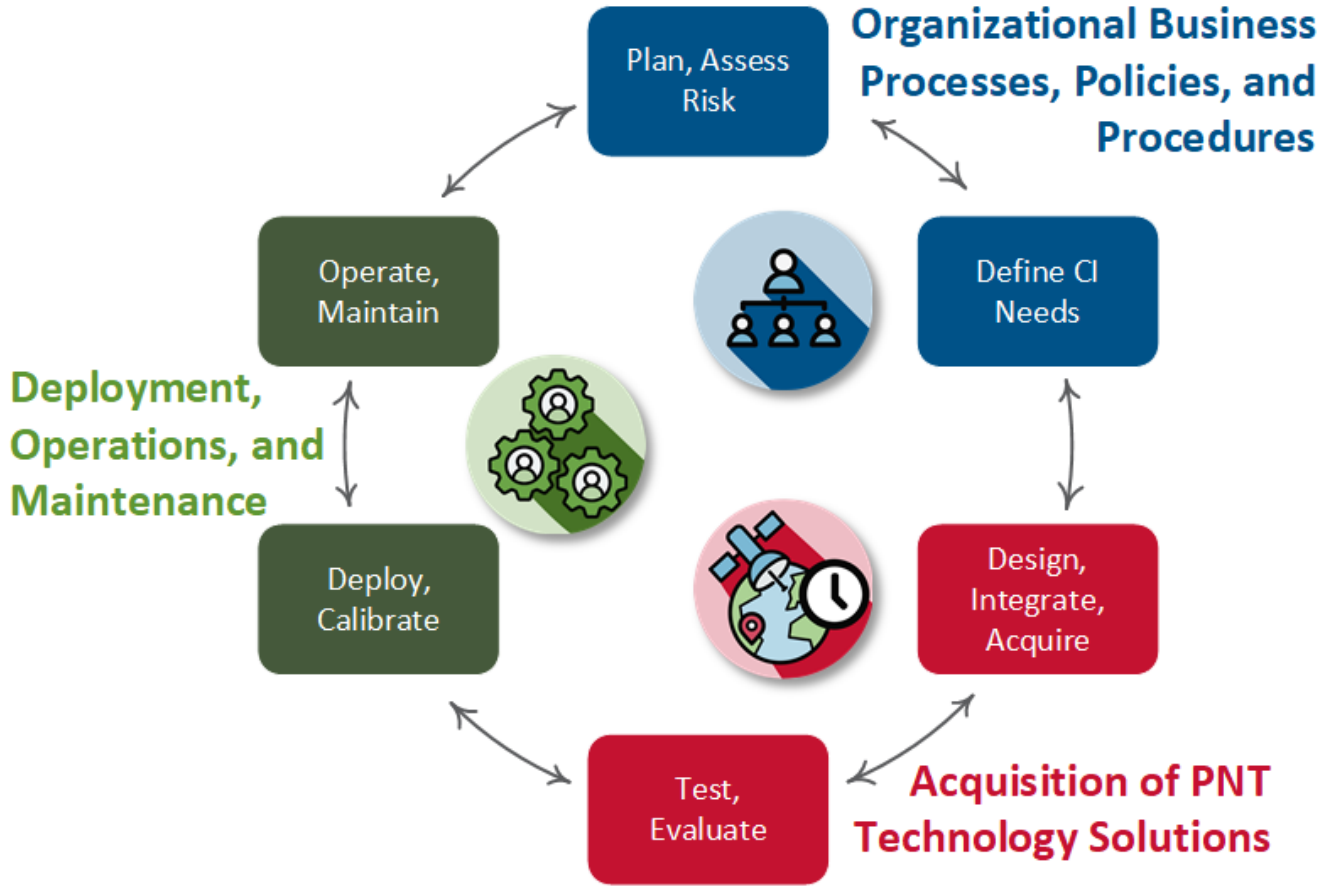
Impact: Adoption of Best Practices furthers the responsible use of PNT in accordance to E.O. 13905 and lowers risk to stakeholder that underpin the nation's critical infrastructure.

Stakeholders:

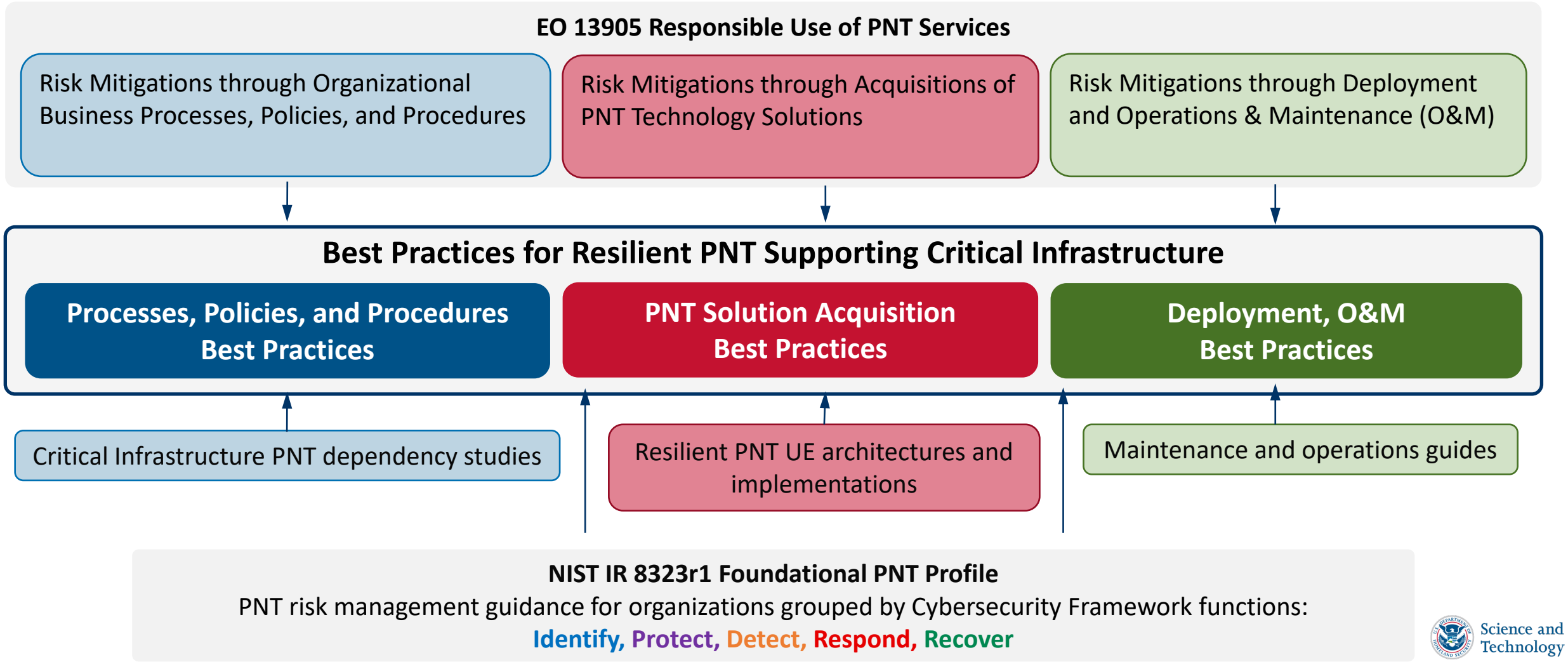
- **CI Owners**
- **CI Operators**
- **Manufacturers and Integrators**
- **Test Industry**
- **PNT Service Providers**

BLUF: This document provides an inclusive guide to PNT Best Practices for organizational policies, technology solutions, and operations and maintenance to implement resilient PNT solutions, supporting the policies set forth by E.O. 13905 and the NIST Foundational PNT Profile.

Risk Mitigation Best Practices Categories for the Responsible Use of PNT



PNT Best Practices
PPD21 – Critical Infrastructure Security and Resilience



Science and Technology

Planning and Risk Assessment Best Practices

- BP-PR 1: Perform a maturity assessment to establish a foundation for responsible use of PNT services and inform RPNT Lifecycle decisions
- BP-PR-2: Assess and mitigate PNT service risk through organizational processes, policies and procedures.
- BP-PR 12: Identify relevant PNT resilience requirements.

PNT Solutions Acquisition Best Practices

- BP-AS 9: Understand relevant threats and ensure PNT equipment has appropriate threat detection and risk mitigation.
- BP-AS 10: Identify appropriate holdover or backup capabilities for PNT systems.

Deployment, Operations, and Maintenance Best Practices

- BP-DO 1: Carefully select antenna locations.
- BP-DO 2: Obfuscate visibility of the primary antenna.
- BP-DO-13: Report suspicious PNT UE events and adverse conditions to appropriate authorities

Engage with us:

scitech.dhs.gov

GPS4Critical-Infrastructure@hq.dhs.gov

@dhsscitech

Science and Technology