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

# Responsible Use of PNT and Department of Homeland Security (DHS) Activities

**Civil GPS Service Interface Committee**

Science and Technology

**Ernest Wong**
PNT Technical Lead
Technology Centers Division
September 12, 2023

# Agenda

- Understanding the “Responsible Use of PNT” Process
- Resilient PNT Capability Maturity Model (RPNT CM2)
- GPS Equipment Testing for Critical Infrastructure (GET-CI) 2024

**Acronyms**

- PNT: Positioning, Navigation, and Timing
- GPS: Global Positioning System
- GNSS: Global Navigation Satellite System
- NIST: National Institute of Standards and Technology
- NIST IR: NIST Internal or Interagency Reports
- NIST SP: NIST Special Publication

# Where does “Responsible Use of PNT” Fit In?

Executive Order (EO) 13905

NIST IR 8323 Foundational PNT Profiles

Resilient PNT Conformance Framework

Resilient PNT Reference Architecture

PNT Federal Contract Language

Responsible Use of PNT

Space Policy Directive (SPD) 7

GPS Best Practices

Space Policy Directive (SPD) 5

Science and Technology

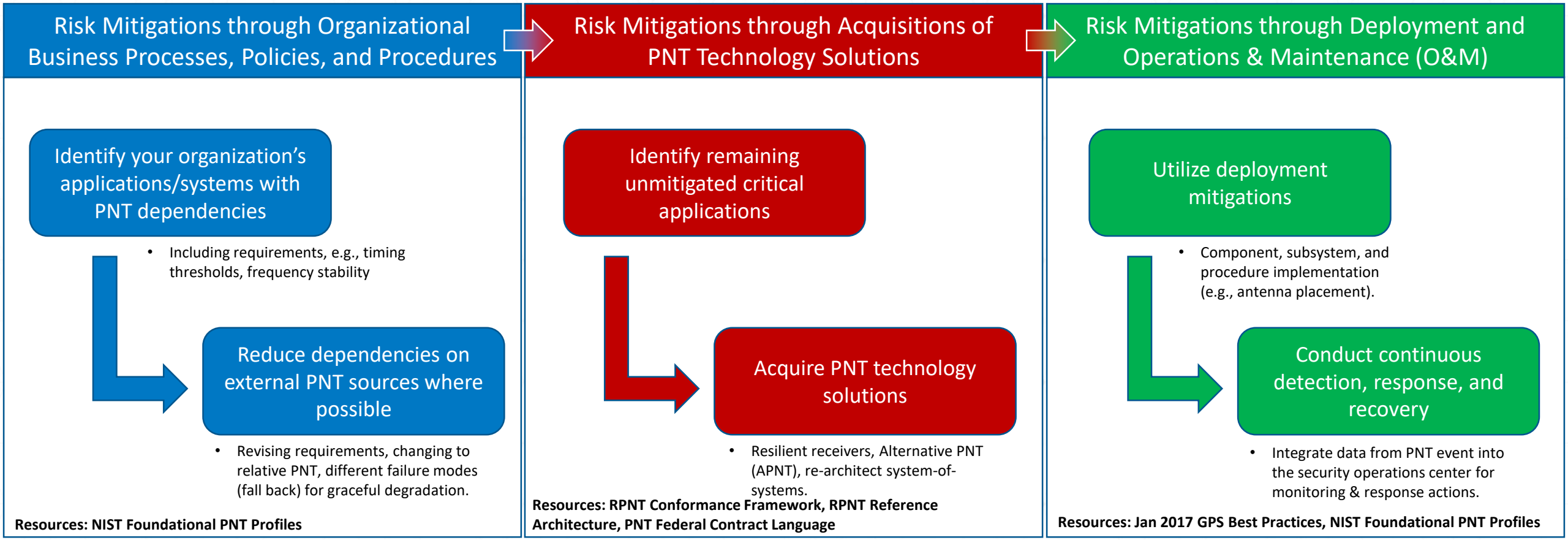
# Responsible Use of PNT

- EO13905 Definition:
  - “Responsible use of PNT services” means 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.

- Main Points:
  - “Responsible Use of PNT” is applied through an organizational risk management process.
  - Technology solutions are *NOT* the first step.
    - Comparison: Cybersecurity awareness training is low-hanging fruit. Technology solutions comes after.

# Process for Applying "Responsible Use of PNT"

- Organizational risk management actions come before technology solutions.
  - Comparison: Cybersecurity awareness training (policy) is low-hanging fruit. Technology solutions comes after organizational maturity.



# Resilient PNT Capability Maturity Model

- Purpose: Develop a capability maturity model for organizations to benchmark and mature their PNT resilience capabilities.
  - Intended to help organizations without PNT expertise to get started on PNT resilience
  - Leverages the NIST Foundational PNT Profile
  - Incorporates “Responsible Use of PNT” concepts

- Enable organizations to do the following:
  1. Inform actions and investments for reaching a target maturity level.
  2. Consistently measure their PNT resilience capabilities
  3. Enhance their PNT resilience posture
  4. Share knowledge

# Resilient PNT Capability Maturity Model (2)

- **Approach**
  - 4 maturity levels (crawl, walk, run)
    - Levels target different NIST Cybersecurity Framework functions (Identify, Protect, Detect, Respond, Recover)
  - Core vs. Electives
    - Allows flexibility and tailoring for organizational focus
    - Core requirements based off NIST PNT Profiles (NISTIR 8323)
    - Elective requirements based off NIST SP 800-160 Vol.2
  - Visualized Reporting Format
    - Decision Support Tool: Help quickly inform decision makers and review organizational posture.
    - Will convey high-level information at-a-glance. Will be similar (conceptually) to traffic light charts.

# Conceptual Preview of Maturity Levels

## Initial Foundation

Level 1

### Identify

**Organizational Planning**

- Understand **general PNT threats**
- **Identify** critical assets dependent on PNT
- **Manual recovery** plan in place for PNT disruptions

## Intermediate

Level 2

### Protect and Detect

**Generalized Mitigations**

- Understand **sector-specific PNT threats**
- **Protect** critical assets dependent on PNT
- **Monitor** for PNT anomalies in dependent systems
- **Partially automated recovery** plan in place

## Advanced

Level 3

### Automate Response

**Minimizing Impacts**

- Assess your **organization-specific PNT threats**
- **Proactive defense & response** to mitigate effects on dependent systems.
- **Automated recovery** that minimizes operational impact.

## Adaptive

Level 4

### Evolve Techniques

**Future-Proofing**

- **Anticipate** emerging PNT threats and risks
- **Tailor** risk mitigations to the organization
- Incorporate **zero-trust resilience techniques**
- **Recover PNT services** w/o service degradation

Note: This is subject to change.

Science and Technology

# GET-CI 2024 Test Event

- **2024 GPS Equipment Testing for Critical Infrastructure (GET-CI 2024)**
  - What: Live-sky GPS spoofing test event for civil industry stakeholders to evaluate their PNT equipment
  - For Who: Equipment manufacturers, critical infrastructure end-users
  - When: Planning for 2nd half of 2024
  - How to apply: RFI for Participation (RFIP) will be posted on SAM.gov
    - RFIP posting is pending
    - When posted, will be findable as News Item on GPS.gov and press release on DHS S&T website

[ SCIENCE AND TECHNOLOGY DIRECTORATE ]

# Engage with us:

scitech.dhs.gov

SandT.Innovation@hq.dhs.gov

@dhsscitech

Science and Technology