# NIST PNT PROFILE: A QUICK GUIDE

**Getting Started with the NIST Foundational Positioning, Navigation and Timing (PNT) Profile**

## What is it?

The NIST Foundational PNT Profile (NISTIR 8323) is a voluntary tool that can help your organization increase its resilience through responsible use of PNT services as described in Executive Order (EO) 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation and Timing Services*.

## What is Responsible Use?

The responsible use of PNT services is defined as 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.

## How can my organization use it?

Organizations can apply this Foundational Profile to their own unique missions, business environments, and technologies to create or refine a security program that will include the responsible use of PNT services. The PNT Profile was created by applying the NIST Cybersecurity Framework (CSF) to help organizations:

- Identify systems dependent on PNT
- Identify appropriate PNT sources
- Detect disturbances and manipulation of PNT services
- Manage the risk to these systems

## The following five key considerations are consistently seen in the PNT profile document and merit strong attention:

**1** Consider performing activities to discover all devices to include PNT services and those hosts that use PNT services. The use of PNT data may not be obvious.

**2** Consider incorporating alternate PNT sources into the business architecture and ensure the ability to fail over to these systems in the event of a disruption.

**3** Consider implementing procedures to detect PNT data manipulation, disruption or other relevant cybersecurity events. Comparison of multiple complementary sources and communication paths for position, navigation, or time may enable the detection of manipulation of PNT services.

**4** Consider developing policies, procedures, and plans to respond to a disruption or manipulation of PNT services.

**5** Consider developing recovery plans to restore systems affected by a PNT service disruption or manipulation to a proper working state.

# NIST PNT PROFILE: A QUICK GUIDE



## Applying the Cybersecurity Framework (CSF) to PNT Services

The Cybersecurity Framework (CSF) provides prioritized, flexible, risk-based, and voluntary guidance, based on existing standards, guidelines, and practices, to help organizations better understand, manage, and communicate cybersecurity risks. The CSF is organized by five high-level functions: Identify, Protect, Detect, Respond, and Recover. These functions provide the basis to develop guidance on cybersecurity risk management as applied to PNT services.

### IDENTIFY

The Identify Function provides key elements which should be given strong consideration in this analysis. Consideration of the threat environment and the organization's purpose, assets, and vulnerabilities will have a significant influence on the overall risk.

Objectives include:

- Identify the business/operational environment and organization's purpose
- Identify all assets, including applications dependent on PNT data
- Identify sources and infrastructure that provide PNT information
- Identify the vulnerabilities, threats, and impact should the threat be realized to assess the risk

### PROTECT

The Protect Function includes the development, implementation, and verification measures to prevent loss of functionality in the case of PNT disruption or manipulation.

Objectives include:

- Protect the systems forming, transmitting, and using PNT data to support the needed level of integrity, availability and confidentiality based on application needs
- Protect the deployment and use of PNT services through adherence to cybersecurity principles, including understanding the baseline characteristics and application tolerances of the PNT sources, data, and any contextual information, providing sufficient resources, managing the systems development life cycle, as well as deploying needed training, authorizations, and access control
- Protect users and applications dependent on PNT data, should a threat be realized, by enabling users and applications to maintain a sufficient level of operations through verified response and recovery plans
- Protect organizations relying on PNT services and data with respect to business and operational needs

### DETECT

The Detect Function addresses the development and deployment of the appropriate activities to monitor for anomalous events and notify downstream users and applications.

Objectives include:

- Enabling detection through monitoring and consistency checking
- Establishing a process for deploying and handling detected anomalies and events

### RESPOND

The Respond Function addresses the development and implementation of the appropriate activities to respond to a detected cybersecurity (and/or anomalous) event. The activities in the Respond Function support the ability to contain the impacts of a potential cybersecurity or anomalous event.

Objectives include:

- Contain PNT events using a verified response procedure
- Communicate to PNT data users, applications, and stakeholders the occurrence and impact of the event on PNT data
- Develop processes to respond to and mitigate new known or anticipated threats and/or vulnerabilities
- Evolve response strategies and plans based on lessons learned

# NIST PNT PROFILE: A QUICK GUIDE



## Applying the Cybersecurity Framework (CSF) to PNT Services

**CONTINUED**

### RECOVER

The Recover Function develops and implements the appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations and return the organization to its proper working state after a disruption or manipulation to PNT services has occurred.

Objectives include:

- Restore systems dependent upon PNT services to proper working state using a verified recovery procedure
- Communicate to PNT data users, applications, and stakeholders the recovery activities and status of the PNT services
- Evolve recovery strategies and plans based on lessons learned

## Bringing it all together.

The PNT Profile categories provide the information your organization needs to undertake the process of managing risks against potential disruption and manipulation of the PNT services, including networks and components that transmit or use PNT data. Specifically, the “Applicability to PNT” column in Section 4 of the PNT Profile contains the intended outcomes of responsible PNT use. Mitigation measures are provided in the reference column to aid each subcategory implementation.