Positioning, Navigation, and Timing (PNT) Profile Development

Executive Order 13905

Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services

Background

- Executive Order 13905 of February 12, 2020

  Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services.

- "Because of the widespread adoption of PNT services, the disruption or manipulation of these services has the potential to adversely affect the national and economic security of the United States. To strengthen national resilience, the Federal Government must foster the responsible use of PNT services by critical infrastructure owners and operators."

Background

EO 13905

- Responsible use of PNT services – deliberate, risk informed use of PNT services
- If disruption or manipulation occurs, minimal impact to national security, economy, public health, and critical functions of Federal Government
- Critical infrastructure – systems/assets so vital to the US that incapacity or destruction could result in debilitating impact

Overview

Several Federal agencies tasked directly

- NIST: create "profile" due within one year (02/12/2021)
- Other agencies to follow on with sector specific profiles
- EO tasking applies to Federal Government, EO intended to benefit both public and private sector

NIST Objectives

- Provide single, foundational profile to include all stakeholders for responsible use of PNT
- PNT Profile focus is on cybersecurity, not operations, although it is understood there will likely be overlap
- Lay groundwork for Sector Specific Agencies (SSAs) to fulfill their requirements to create sector specific profiles

NIST Objectives

- Engage with primary stakeholders public and private (coordination with GPS.gov program office and eager to talk to more)
- Focus on critical infrastructure, namely - owner/operators of the electrical power grid, communication infrastructure, businesses in the transportation, agriculture, weather, and emergency response sectors, among others
- Leverage the Cybersecurity Framework to develop and issue a foundational PNT profile

NIST Request for Information (RFI)

- RFI seeks information from PNT technology vendors, users of PNT services, and other key stakeholders for the purpose of gathering information to foster the responsible use of PNT services.
- RFI responses, in addition to continued stakeholder engagement, will be used to inform and create profile.

NIST Request for Information (RFI)

- Describe any public or private sector need for and/or dependency on the use of positioning, navigation, and timing, or any combination of these services.
- Identify and describe any impacts to public or private sector operations if PNT services are disrupted or manipulated.

NIST Request for Information (RFI)

- Identify any standards, guidance, industry practices and sector specific requirements referenced in association with managing public or private sector cybersecurity risk to PNT services.
- Identify and describe any processes or procedures employed by the public or private sector to manage cybersecurity risks to PNT services.

NIST Request for Information (RFI)

- Identify and describe any approaches or technologies employed by the public or private sector to detect disruption or manipulation of PNT services.
- Identify any processes or procedures employed in the public or private sector to manage the risk that disruption or manipulation to PNT services pose.

NIST Request for Information (RFI)

- Identify and describe any approaches, practices, and/or technologies used by the public or private sector to recover or respond to PNT disruptions.
- Any other comments or suggestions related to the responsible use of PNT services.

NIST Request for Information (RFI)

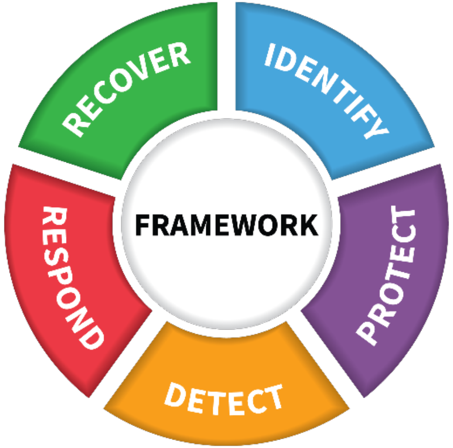
- Stakeholders can submit responses to NIST via:
  - regulations.gov
  - pnt-eo@list.nist.gov

- All responses will be posted publicly on
  - https://www.nist.gov/itl/pnt

PNT Profile Development Process

- Open, transparent, and collaborative
- Profile will provide guidance to organizations on how to:
  - ❑ Identify systems dependent on PNT
  - ❑ Identify appropriate PNT sources
  - ❑ Detect disturbances and manipulation of PNT services
  - ❑ Manage the risk to these systems

Cybersecurity Framework



- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Meant to be paired
- Living document
- Guided by many perspectives – private sector, academia, public sector

Cybersecurity Framework Profiles – Examples

https://www.nist.gov/cyberframework/resources/risk-management-resources

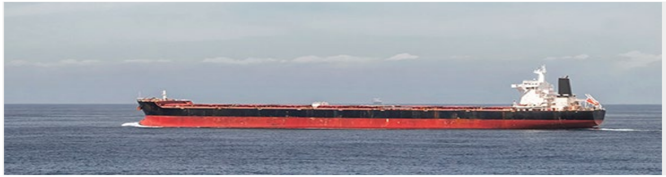
Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Financial Services Profile

Financial Services Sector Specific Cybersecurity "Profile"

FSSCC



Maritime Profile

Bulk Liquid Transport Profile

Planned Timeline

- RFI response period opened **05/27/2020**, for a 45 day comment period
- Initial analysis of RFI responses anticipated: **August 2020**
- Issue PNT Profile draft annotated outline: **Summer 2020**
- Host PNT Profile status update webinar: **Summer 2020**
- Issue draft PNT profile for public comment: **Fall 2020**
- Host PNT profile status update webinar: **Fall 2020**
- Issue final PNT Profile: **February 12, 2021**

Executive Order 13905 Sec. 4i:

Within 180 days of the date of this order, the Secretary of Commerce shall make available a GNSS-independent source of Coordinated Universal Time, to support the needs of critical infrastructure owners and operators, for the public and private sectors to access.

- Working with outside stakeholders to deliver GNSS-independent UTC with an accuracy required for critical infrastructure.
- First inquiries were to develop timing delivery over optical fiber.
- Will work with interested parties to explore other technology as well.
- **Due by 8/10/20**

STAY IN TOUCH

Questions can be submitted via email or on Twitter!

✉ Email:
pnt-eo@list.nist.gov

@NISTcyber
Use #NISTPNT

The webcast recording will be posted at 2PM EDT on June 4th.