Positioning, Navigation, and Timing (PNT) Profile Development

Executive Order 13905

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

Welcome

- NIST wants to hear from the private sector, academia, and industry
- This is a priority - it is what drives this work
- These unique times require a different approach but our goal, as always, is to listen to stakeholders
- In the end, what is success?

Agenda

Welcome / Opening Remarks	Matt Scholl, NIST
Keynote	Brian Cavanaugh, NSC
NIST Task / Process	Jim McCarthy, NIST
PNT Primer	Arthur Scholz, PhD, MITRE Corp.
CSF and CSF Profile Primer	Kevin Stine, NIST
Next Steps / Closing Remarks	Jim McCarthy, NIST

Keynote

Brian Cavanaugh, EOP/NSC

Special Assistant To The President and Senior Director for Resilience Policy at National Security Council,

The White House

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/Scope

- 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/Scope

- 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

PNT Definitions

- PNT services: any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof.
- Profiles as defined in EO: a description of the responsible use of PNT services — aligned to standards, guidelines, and sector-specific requirements — selected for a particular system to address the potential disruption or manipulation of PNT services.

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

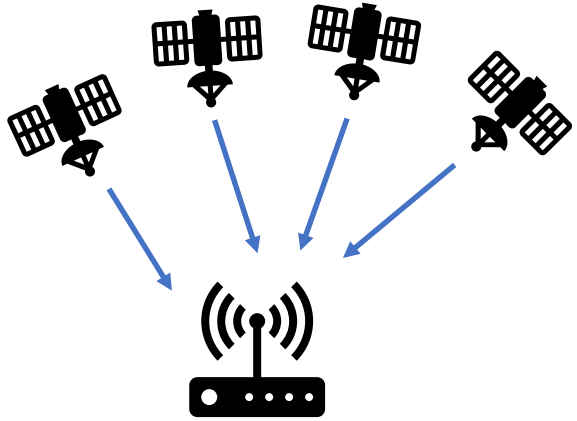
Positioning, Navigation, and Timing

- **Where am I?**
- **How do I get from here to there?**
- **What time is it?**

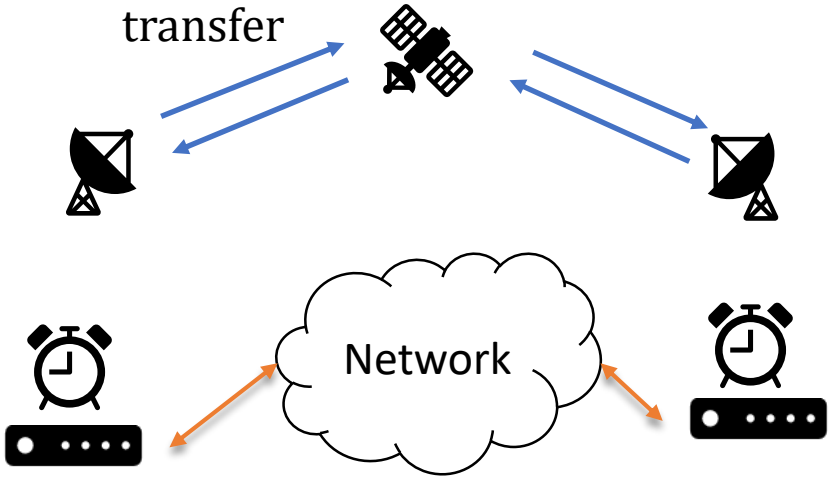
https://www.transportation.gov/pnt/what-positioning-navigation-and-timing-pnt

PNT Services

- Broadcast Systems:
  - Receivers only listen
  - Service has unlimited capacity



- Two-way Systems
  - Limited Capacity
  - Often used for precision time transfer



Is it PNT or GPS?

- Global Navigation Satellite Systems (GNSS) have become synonymous with PNT
  - The Global Positioning System (GPS) is the oldest and most widely used GNSS
- GNSS receivers have largely replace relative and legacy systems
  - Free
  - Global coverage
  - Better accuracy and precision than most application require
- Other methods still required in GNSS challenged environments
  - GNSS receivers have vulnerabilities
  - Alternative PNT and complementary PNT systems are in development

GPS is often used out of convenience rather than performance requirement.

Responsible Use of PNT Services

- Do you fully understand your reliance and dependence on different PNT technologies?
- Do your systems have adequate robustness and fallback capabilities?

Resources:

- Improving the Operation and Development of GPS Equipment Used by Critical Infrastructure
  https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf
- Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations
  https://www.us-cert.gov/sites/default/files/documents/Best%20Practices%20-%20Time%20and%20Frequency%20Sources%20in%20Fixed%20Locations_S508C.pdf
- Time – The Invisible Utility
  https://www.us-cert.gov/sites/default/files/documents/Corporate_Leadership_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf
  https://www.us-cert.gov/sites/default/files/documents/Technical-Level_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf

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 Components

Core

Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Implementation Tiers

A qualitative measure of organizational cybersecurity risk management practices

Profiles

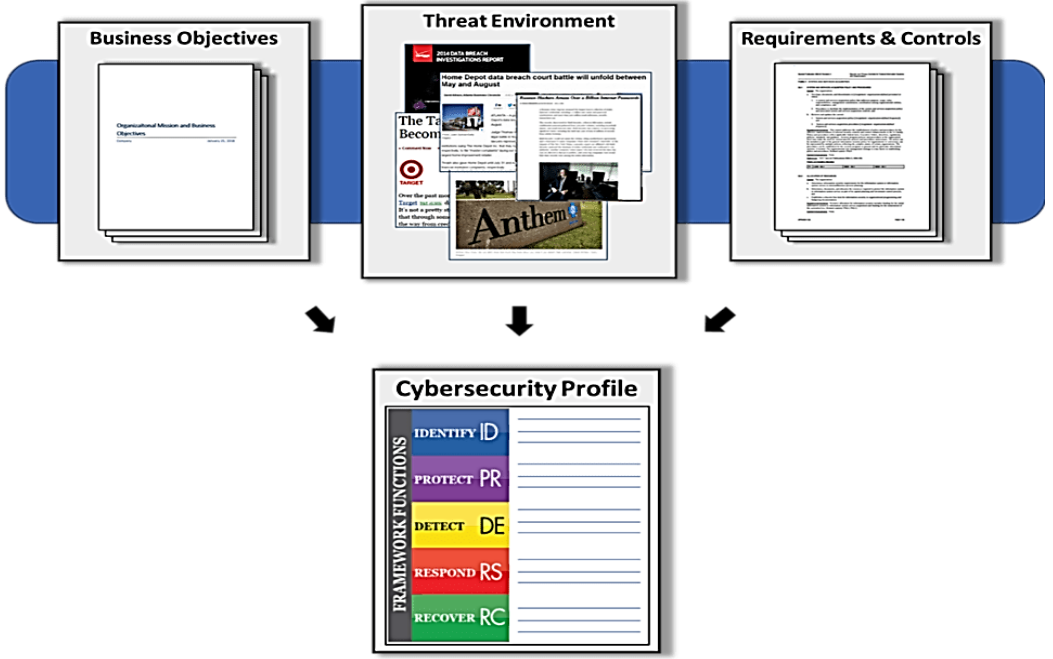
Alignment of an organization's requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core

Cybersecurity Framework Components: Core

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Cybersecurity Framework Components: Profile



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"

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**

WRAP UP

Please remember to submit RFI responses during the 45 day comment period which started 05/27/2020

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.