National Institute of Standards and Technology
U.S. Department of Commerce

NIST Workshop:
Responsible Use of Positioning, Navigation and Timing (PNT) Services

September 15, 2020

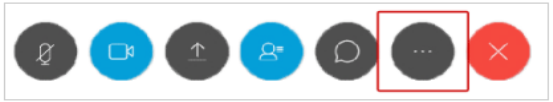
Engage with us

Please share your questions via the Q&A panel on the Webex Platform

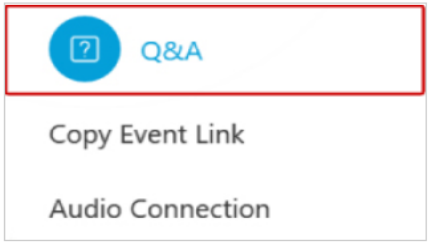
Q&A

How to find

1 In the toolbar at the bottom, click on the 3-dot button



2 On the menu, click Q&A



3 Type your question in the box

4 Click **send** or **send privately**

Agenda

Welcome / Opening Remarks	Matt Scholl, NIST
PNT Profile Overview	Jim McCarthy, NIST
CSF and CSF Profile Primer	Kevin Stine, NIST
Annotated Outline Overview	Joe Brule, NSA
Break	
Panel Discussions	
1:00pm EDT	Industry Panel
2:00pm EDT	Federal Panel

Overview of PNT Profile Development

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

Tasks

- 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

Overview

NIST Objectives

- Provide single, foundational profile to support a wide range of stakeholders on the responsible use of PNT
- PNT Profile focus is on cybersecurity
- Lay groundwork for Sector Specific Agencies (SSAs) to fulfill their requirements to create sector specific profiles

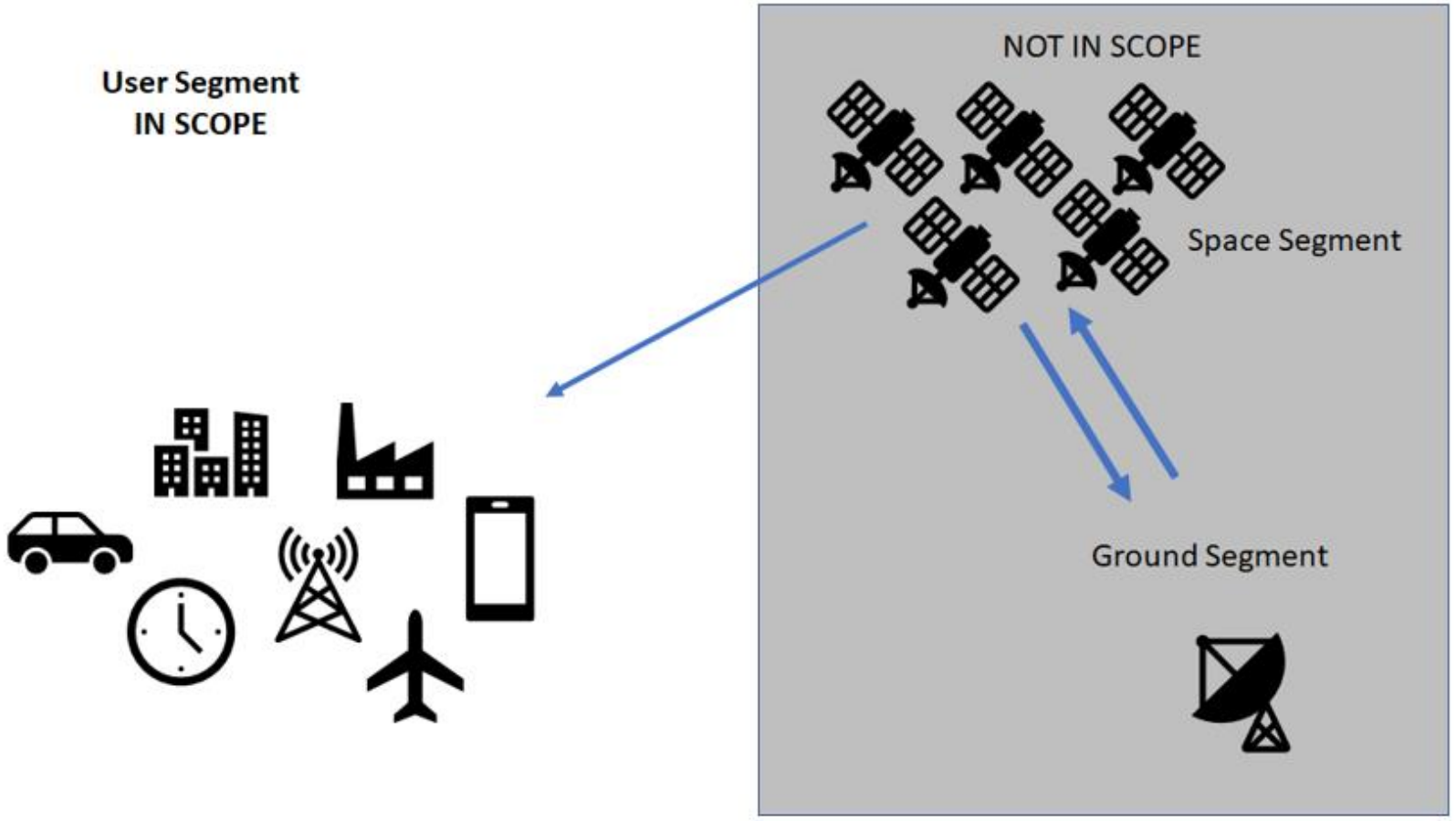
Overview

NIST Objectives

- Engage with primary stakeholders, both public and private, to inform development of the PNT profile
- Focus on Critical Infrastructure - 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

Overview

NIST Profile Scope



Summary of Profile Development Activities

NIST Public Engagement Activities to Date

- Issued Request for Information (RFI) 05/27/2020. RFI responses closed 07/13/2020.
- PNT EO Virtual Webinar presented by NIST to PNT stakeholders 06/04/2020
- NIST releases annotated outline describing contents of what will be in the PNT profile - 09/03/2020
- PNT Webinar - 09/15 & 09/16 - comprehensive update and live sessions to further inform and enhance development of PNT profile

Overview

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.

Overview

PNT Profile Development Process

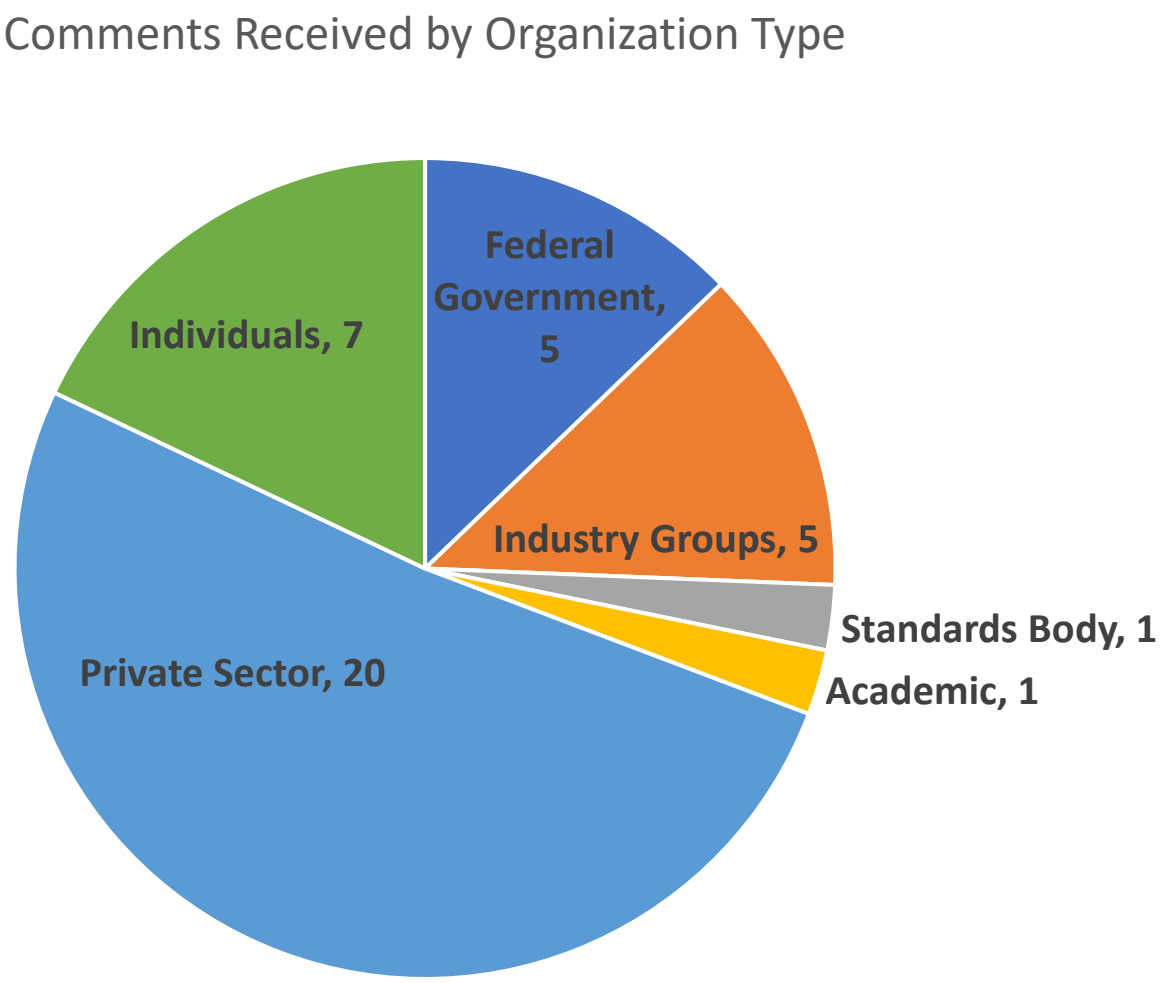
- Open, transparent, and collaborative

- 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

RFI Response Overview

Total Number of Responses:

39



RFI Response Overview - Themes

Key Themes from RFI Responses:

- **Dependencies**
  - ❑ Vital business need for tracking, monitoring, and positioning of assets
  - ❑ Precise timing necessary for coordinating asset activity/monitoring across multiple sites
- **Potential Disruptions**
  - ❑ Manipulation – spoofing
  - ❑ Denials of signal (natural or technical)
- **Impact of Disruptions**
  - ❑ Degradation of services
  - ❑ Operational Risks
- **Mitigation** strategies
  - ❑ Monitor RF
  - ❑ Use alternate source(s)
  - ❑ Carry over (temporary)
  - ❑ Accept Risk
- **Sectors**
  - ❑ Energy
  - ❑ Aviation
  - ❑ Communications
  - ❑ Public Safety
  - ❑ Underwater drilling
  - ❑ Automotive
  - ❑ Agriculture

Overview

PNT Profile Development Timeline

February 12,2020
PNT Resiliency Executive Order Published

Spring 2020
NIST Request for Information issued; hosted initial PNT profile webinar

Summer 2020
Draft annotated outline published; profile development workshop convened

Fall 2020
Draft PNT profile published; open for public comment

February 12, 2021
Final PNT profile published

Questions?

Please share your questions via the Q&A panel on the Webex Platform

Overview of NIST Cybersecurity Framework

NIST 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

NIST Cybersecurity Framework

Three Primary 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

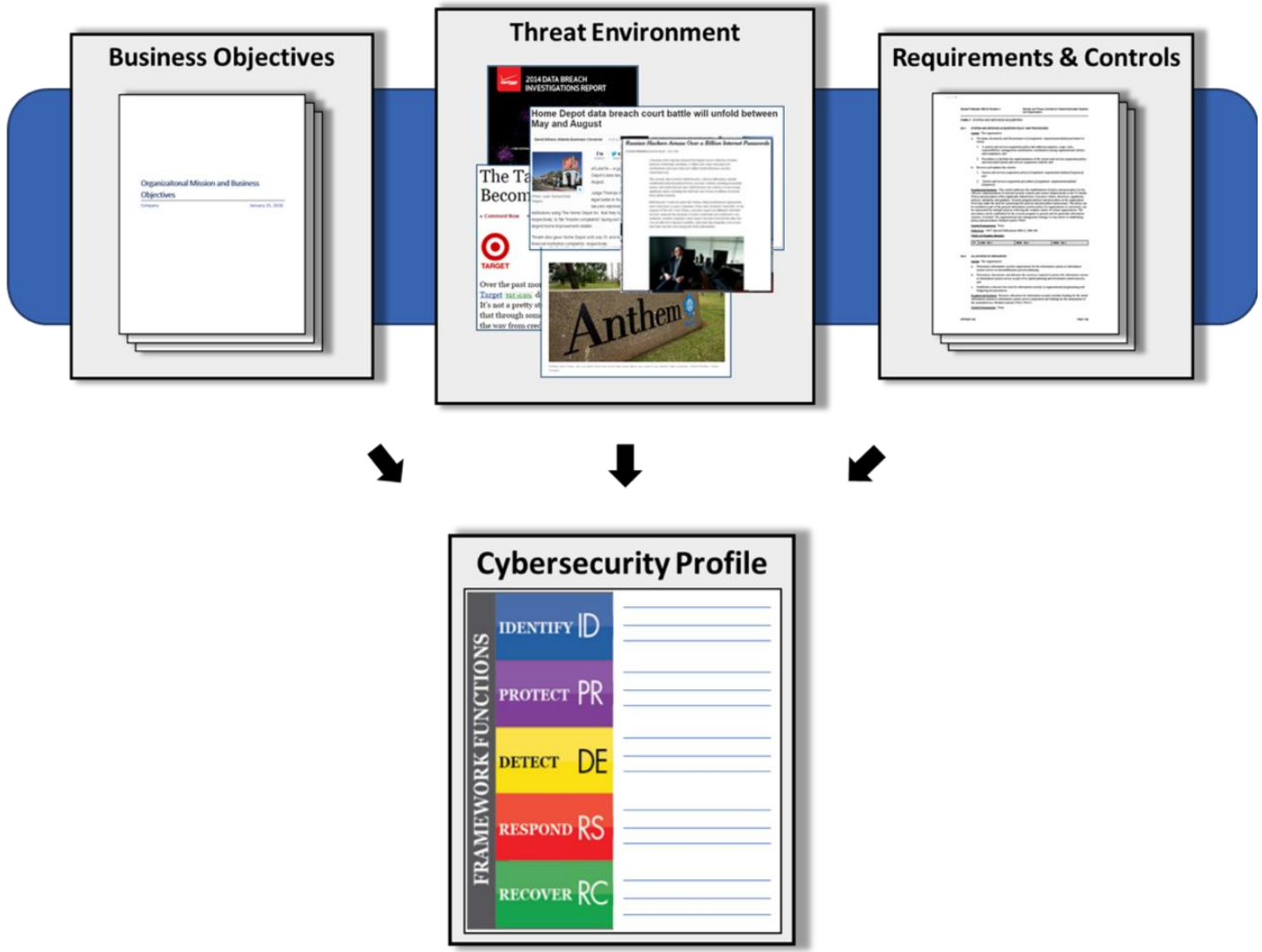
Framework Core

Establishes a Common Language

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 Profiles



Cybersecurity Framework Profile - Examples

Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Cybersecurity Framework Smart Grid Profile

Cybersecurity Framework Smart Grid Profile

Maritime Profile

Bulk Liquid Transport Profile

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

Questions?

Please share your questions via the Q&A panel on the Webex Platform

Overview of PNT Profile Annotated Outline

What could Possibly Go Wrong?

- Portions of the Critical Infrastructure Require PNT Data and Services
- Heavy Reliance on a single PNT Service Provider
- Increased Impact and/or Increased Threat Leads to Increased Risk

Bottom Line Up Front:

- Use the CSF to create a risk based cyber security approach
- Facilitate responsible use of systems that form or use PNT data
- Annotated Outline provides insight into the direction of the PNT profile based on NIST's analysis and synthesis of the RFI responses
- Panel Discussions, Breakout Sessions will provide NIST with your insights

PNT Profile: Target Audience

Target Audience:

- Organizations that use PNT services
- Managers responsible for the systems that form or use PNT data
- Risk managers/ cyber security professionals
- Procurement officials
- Mission and business owners
- Researchers

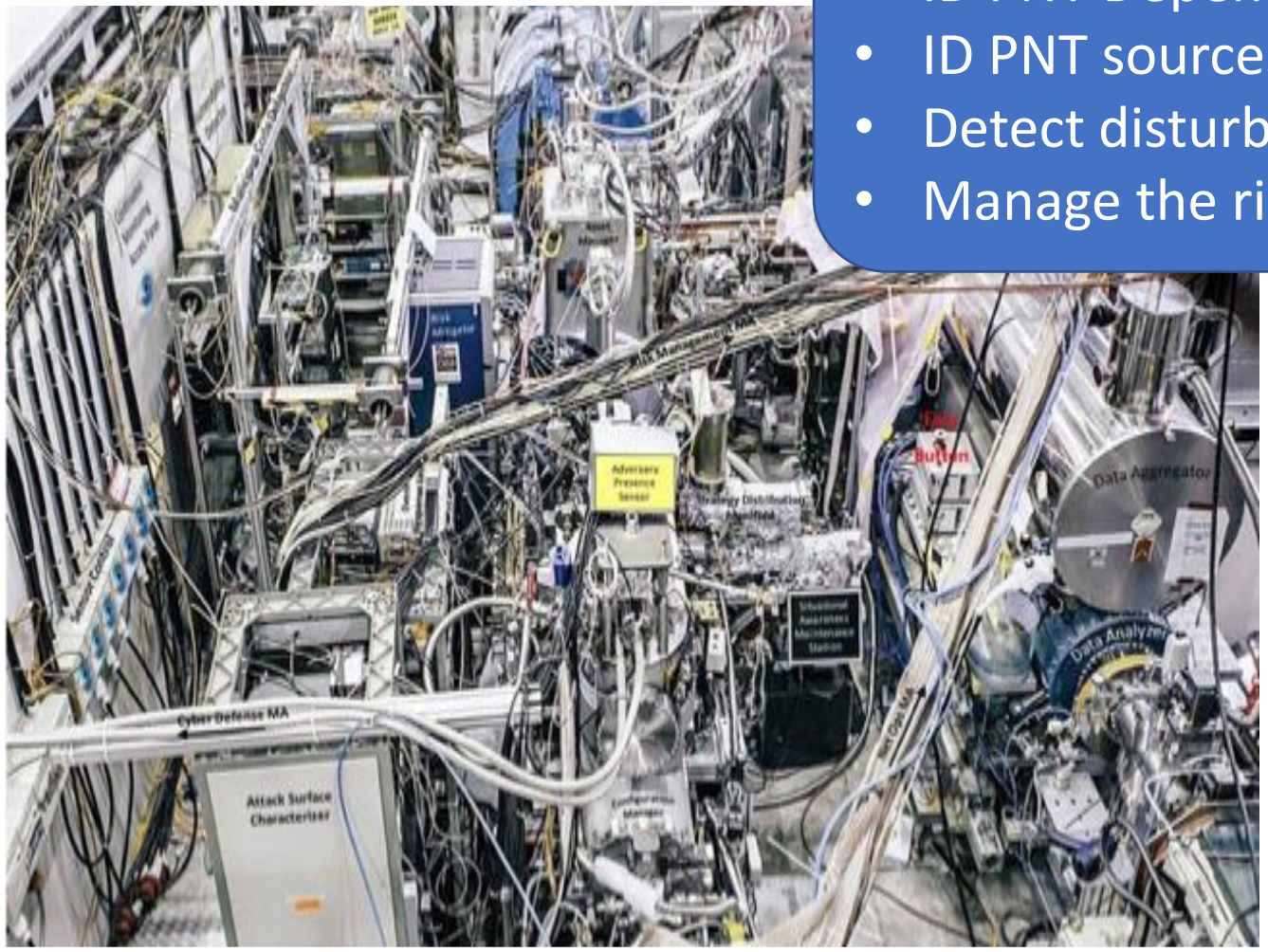
PNT Profile: Purpose and Objectives

- Purpose of the Profile is to Provide *Guidance* to Stakeholders Who Intend to Establish a Risk Management Approach to PNT Resiliency
  - Not a 'Checklist'
  - Advisory, Not Regulatory
- Objectives Include:
  - Identify systems that form or use PNT data
  - Identify PNT sources
  - Identify and share information about common threats and mitigation strategies
  - Protect PNT Services
  - Detect anomalies and outages
  - Assess and manage risk in the event of a PNT degradation or outage
  - Respond to anomalies in a manner consistent with Risk Management Principles

The CSF Enables EO 13905

EO 13905 :

- ID PNT Dependencies
- ID PNT sources
- Detect disturbances & manipulation
- Manage the risk



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

What Is Accomplished by Using the PNT Profile?

The PNT Profile is intended to:

- Facilitate responsible use of the systems that form or use PNT data
- Apply the CSF in the context of PNT Data Use/Reliance
  - Development of policies and procedures for PNT data risk identification, protection, detection, response, and recovery
- Assist an organization's PNT-related Risk Management efforts
- Help organizations develop sector-specific PNT profiles
- Prioritize PNT-related cybersecurity measures in accordance with business or mission objectives
- Use recommended policies and procedures for the acquisition, integration, and deployment of applications and systems forming and using PNT data

Draft Overview of the PNT Cybersecurity Profile

The Profile's Annotated Outline Highlights these Areas:

- Risk Management Overview
- Resilience – Key Theme in the E.O.
- Capabilities Overview
  - Policy and Procedures
  - Technical Capabilities

PNT Profile - Maps to the components of the CSF to enable users of the systems that form or use PNT data to employ effective Risk Management practices for PNT data and critical infrastructure resiliency

  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

Questions?

Please share your questions via the Q&A panel on the Webex Platform

Responsible Use of PNT Services

Identify systems using PNT services	• Well-characterized application requirements • Documentation and calibration of systems using PNT data • Scheduled maintenance • Regular verification and validation of components
Identify appropriate PNT sources	• Integration of diverse and/or complementary PNT sources • Documentation and calibration of systems forming PNT data • Scheduled maintenance • Regular verification and validation of components
Detection of disturbances	• Signals of opportunity: cross-checking between multiple sources • Situational awareness: continuous monitoring
Risk management	• Integrity protection of the PNT data flow • Timely, effective communications of PNT service disruptions, data quality degradations, and vulnerabilities • Continuous anticipation of novel threat models, security improvement

National Institute of Standards and Technology
U.S. Department of Commerce

NIST PNT Workshop

Private Sector Panel Discussion

September 15, 2020

Private Sector Panel Discussion

Panelists

Michael Calabro
Chief Engineer, Booz Allen Hamilton
Vice Chair, Synchronization Committee
Alliance for Telecommunications
Industry Solutions (ATIS)

John Fischer
Vice President
Advanced Research and Development
Orolia

Michael Lewis
Policy and Framework Advisor, Information Risk
Strategy and Management, Chevron
Lead, Information Technology Security Subcommittee
American Petroleum Institute (API)

Gerardo Trevino
Technical Leader, Cybersecurity
Power Delivery and Utilization
Electric Power Research Institute
(EPRI)

Moderator

Suzanne Lightman
Senior Information Security Advisor
National Institute of Standards and Technology

National Institute of Standards and Technology
U.S. Department of Commerce

NIST PNT Workshop

Public Sector Panel Discussion

September 15, 2020

Public Sector Panel Discussion

Panelists

Karen Van Dyke
Director
Position, Navigation and Timing and
Spectrum Management
Department of Transportation

Jim Platt
Chief
Strategic Defense Initiatives
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Evan Dill
Deputy Branch Head
Safety Critical Avionics Systems
Langley Research Center
National Aeronautics and Space Administration

Moderator

Arthur Scholz
Principal Signal Processing Engineer
The MITRE Corporation