Department of Transportation
Office of the Secretary
Office of the Assistant Secretary for Research and Technology (OST-R)

U.S. Dept. of Transportation Update

CGSIC Plenary

September 21, 2021

Assured PNT: Embrace PTA Principle

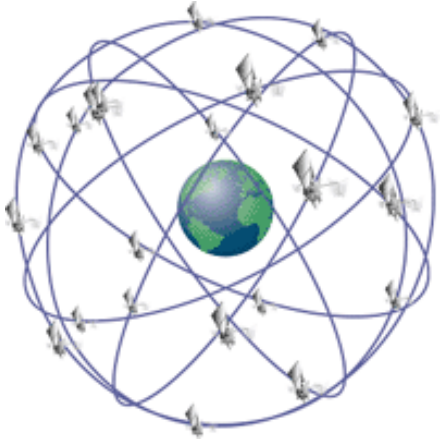
- **Protect**
  - Ensure performance monitoring of space-based civil PNT services
  - Facilitate international coordination for development of monitoring standards
  - Implement interference monitoring capabilities to identify, locate, and attribute PNT threats
  - Prevention of harmful interference
- **Toughen**
  - Authenticate signals and harden user equipment (receiver/antenna/algorithms)
- **Augment**
  - Implement and utilize GPS augmentations and Complementary PNT services

SPD-7 Implementation Plan - DOT Responsibilities

DOT is the lead department for civil PNT, and is responsible for coordinating, defining, and validating requirements for civil applications. DOT represents all civil departments and agencies in GPS development, acquisition, management, and operations.

To implement SPD-7, DOT responsibilities are grouped under the following categories:

- Space-Based PNT Requirements for Civil Applications
- Space-Based PNT Management and Modernization for Civil Applications
- Performance Monitoring and Interference Detection for Civil Space-Based PNT Services
- PNT Resiliency
- Space-Based PNT Data and Signal Authentication
- International Engagement



Executive Order 13905

- **Engage Public and Private Sectors to identify and promote the responsible use of PNT services.**
  - It is the policy of the United States to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure.
  - The Federal Government must increase the Nation's awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services, and it must ensure critical infrastructure can withstand disruption or manipulation of PNT services.
  - To this end, the Federal Government shall engage the public and private sectors to identify and promote the responsible use of PNT services.

EO 13905 Implementation – DOT Activities

Planned Activities:

a. PNT Profile tailoring for transportation applications

b. PNT vulnerability assessment and testing

c. Development of form/fit/function requirements on Ready Reserve Fleet (MARAD) PNT sensor suite based on results based on the DOT Pilot Program

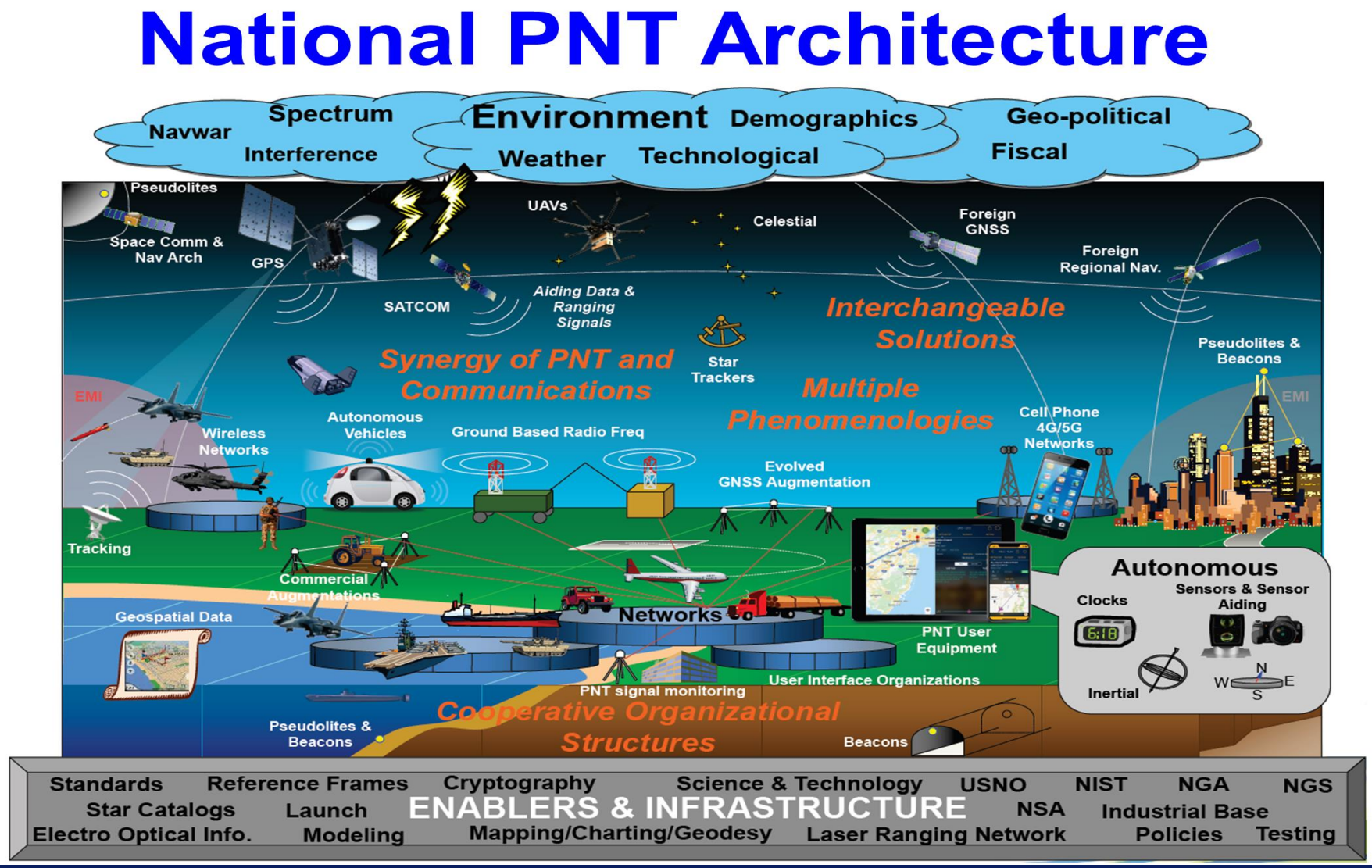
d. Implementation of the goals and objectives of the OSTP R&D Plan for PNT Resilience

National R&D Plan for PNT Resilience

		DHS	DOC/NIST	DOC/NOAA	DOI/USGS	DOT	NASA
Characterize and Model	Characterize PNT system requirements	•		•	•	•	•
	Improve test capabilities and test protocols for assessing equipment and services			•	•	•	•
	Conduct modeling, simulation, and testing to assess vulnerabilities	•			•	•	•
	Develop tools to identify appropriate sources of PNT service based on functional requirements				•	•	•
Improve and Expand	Improve PNT holdover capabilities		•	•	•	•	•
	Develop and improve external sources of additional PNT services	•	•	•	•	•	•
	Establish calibration and traceability techniques		•	•	•		
	Improve and expand disruption detection tools and mitigation methods	•		•		•	•
	Prototype and demonstrate new PNT services	•	•			•	•
Integrate and Deploy	Determine concepts and techniques for securely integrating multiple sources of PNT service	•	•			•	•
	Common hardware platforms	•				•	•
	Develop resilient PNT system architectures	•	•		•	•	•
	Investigate operating internal sources as primary sources of PNT service	•	•	•		•	•
	Develop cybersecurity standards, best practices, and other guidance	•	•		•	•	•

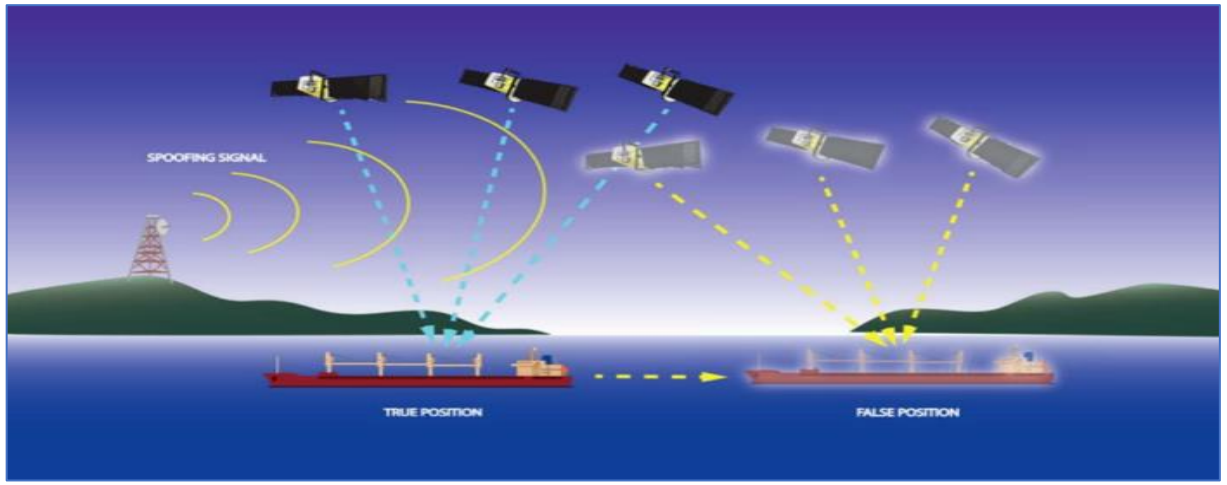
National R&D Plan for PNT Resilience Issued By OSTP on January 20, 2021: Presents a national plan of research and development to improve the resilience of positioning, navigation, and timing services and the critical infrastructure that depends on such services.

National R&D Plan for PNT Resilience



DOT Pilot Program Overview

- Focus on addressing GPS jamming and spoofing impacting maritime vessels:
  - Conduct stakeholder engagement
  - Evaluate Complementary PNT technologies suitable for the maritime environment
  - Develop a jamming and spoofing detection capability



- Results will provide insights to support the development of PNT profiles for maritime applications, as well as to inform additional PNT R&D

GPS Jamming and Spoofing in the Maritime Environment

- DOT public workshop held December 3, 2020
- 426 Registrants
- USG Briefers: NSC, OST-R, MARAD, USCG, Volpe Center
- Industry Briefers: Maersk, APL Maritime, RNT Foundation
  - Operational experience/impacts from GPS jamming and spoofing

Presentations available at:
https://www.transportation.gov/pnt/agenda-virtual-workshop-gps-jamming-and-spoofing-maritime-environment

Results and lessons learned may benefit PNT resiliency for other modes of transportation (aviation, rail, vehicles, and pipeline)

GPS Backup/Complementary PNT Demonstration

- Awarded 11 PNT technology vendor demonstration contracts on rapid acquisition purchase orders through OST-R/Volpe Center
  - Technologies included: Terrestrial RF, Low Earth Orbit, Fiber Optic, and Map Match
- Executed three field campaigns, technology demonstration, and analysis and assessment of data
- Report to Congress submitted on January 15, 2021 (along with NTRSA Report)

PNT Technology Vendor Participation

Vendor	Technology	Site	Timing Scenarios					Positioning Scenarios			
			Demo Site	72-Hr Bench Static Timing	Static Outdoor Timing	Static Indoor Timing	Static Basement Timing	Reference Station Offset (eLORAN Timing)	Dynamic Outdoor Positioning with Holds	Static Outdoor Positioning	Static Indoor Positioning	Airborne 3D Positioning
Echo Ridge LLC	LEO commercial S-band (2483.5 - 2500 MHz)	LaRC					N/A		X		
Hellen Systems, LLC	eLORAN terrestrial RF (90-110 kHz)	JBCC	X			X	X				
NextNav LLC	UHF terrestrial RF (920 - 928 MHz)	LaRC	X	X	X	X	N/A	X	X	X	X
OPNT B.V.	fiber optic time service (white rabbit PTP)	LaRC	X				N/A				
PhasorLab Inc.	802.11 terrestrial RF (2.4 GHz)	JBCC	X	X	X		N/A	X	X		X
Satelles, Inc.	LEO commercial L-band (1616 - 1626.5 MHz)	JBCC	X	X	X	X	N/A		X		
Serco Inc.	R-mode terrestrial RF (283.5 - 325 KHz)	JBCC					N/A	X	X		
Seven Solutions S.L.	fiber optic time transfer (white rabbit PTP)	LaRC	X				N/A				
Skyhook Wireless, Inc.	802.11 terrestrial RF (900 MHz, 2.4 & 5 GHz)	LaRC					N/A	X	X	X	X
TRX Systems, Inc.	UWB & IMU map matching (3.1 - 5 GHz)	LaRC					N/A	X*	X	X	
UrsaNav Inc.	eLORAN terrestrial RF (90 - 110 kHz)	JBCC	X		X	X	X				
GPS (SPS PS)	MEO government L-band (1575, 1227, 1176 MHz)	All	X	X			X	X	X		X

*static holds only

Key: N/A Technology incompatible with scenario definition

Government Host Platforms, 2D and 3D

Fourteen Measures of Effectiveness (MoEs): 1-9: More Quantitative Capabilities

1. Technical Readiness: System (TRL 6-9)
2. Technical Readiness User Equipment (TRL 6-9)
3. Timing and Positioning Accuracy (meters, nanoseconds)
   - Largest 95% bound across the runs in a scenario
4. Spectrum Protection (protected, owned, leased, shared)
5. Service Deployment Effort (low, medium, high)
6. Service Coverage per Infrastructure
   - Count, e.g. number of transmitters, per unit coverage area
7. Service Synchronization (UTC, cascade, self-synchronizing)
   - Timing: UTC, cascade, self-synch
8. PNT Signal Robustness (strong, weak)
   - Emitted power limits, propagation loss, environments
9. Service Resilience (fail-safe, -over, -soft, -hard)
   - System response to changing or off-nominal operating conditions

Fourteen Measures of Effectiveness (MoEs): 10-14: More Qualitative Capabilities

10. PNT Distribution Mode (terrestrial RF, orbital RF, fiber, database)
    - Basic indicator/qualifier on information security

11. Interoperability (high, low)
    - Common platform, in-band/out-of-band, layered components
    - Compatibility with GPS user equipment

12. PNT Information Security (low, medium, high)
    - Authentication, encryption, open
    - Broadcast, point-to-point, controlled access, monitoring

13. Time to Implement Service (short, medium, long)
    - Infrastructure, standards, equipage

14. System/Service Longevity (short, medium, long)
    - Operational life of infrastructure
    - Compatibility with other PNT services & standards
    - Spectrum policy stability

PNT Technology Timing and Positioning Accuracy

	Timing Scenarios					Positioning Scenarios			
Vendor	*72-Hr Bench Static Timing*	*Static Outdoor Timing*	*Static Indoor Timing*	*Static Basement Timing*	*Reference Station Offset (eLORAN Timing)*	*Dynamic Outdoor Positioning with Holds*	*Static Outdoor Positioning*	*Static Indoor Positioning*	*Airborne 3D Positioning*
Echo Ridge					N/A		333.2		
Hellen Sys	114.9			DNC	3.4				
NextNav	23.1	7.1	5.8	17.5	N/A	15.6	6.7	8.9	3.8
OPNT*	0.2				N/A				
PhasorLab	9.4	17.4	18.7		N/A	11.7	7.4		8.6
Satelles	75.5	75.0	9.0	117.0	N/A		9.0		
Serco					N/A	DNQ	39.4		
Seven Soln*	0.1				N/A				
Skyhook					N/A	7.6	1.8	23.5	14.6
TRX					N/A	9.7	6.2	9.8	
UrsaNav	80.1		57.4	DNC	9.7				
GPS (SPS PS)	30	30			30	5	5		7

Rubric:

positioning: max 95%{runs} (m)

1.0

to

350

timing: max 95%{runs} (ns)

0.1

to

120

*1 pps from USG at measurement node

Observations from the FY18 NDAA PNT Demonstration

- FY'18 NDAA GPS Backup and Complementary PNT Demonstration results indicate there are suitable and mature private-sector PNT technologies that have the potential to meet a diversity of application-specific needs.

- The FY'18 NDAA demonstration was designed to showcase technologies in the "best light" possible
  - Complementary PNT technologies were not stress-tested.

- The transportation sector has some of the most stringent PNT performance requirements in terms of accuracy, integrity, availability, and reliability.
  - Not all safety-critical transportation requirements may be met by market-based business models for PNT technologies.

- Private-sector Complementary PNT technologies do not currently have the level of open specifications and standards that have made GPS such a critical and widely adopted service.
  - A similar level of standards, resiliency and vulnerability testing, and performance monitoring must be developed for these technologies.

Complementary PNT: Recommended Next Steps

1. Safety-critical PNT requirements and standards development for transportation services

2. PNT vulnerability and performance testing framework for demonstrated and suitable complementary technologies
   - Procedures, facilities, and platforms for testing PNT performance and resilience to threats
   - Certification protocols for safety-critical PNT functions

3. PNT performance monitoring capabilities to ensure operational PNT services provide resilience and achieve safety-critical standards for transportation and critical infrastructure applications

Center of Automated Vehicles Research with Multimodal AssurEd Navigation (CARMEN) – Initiated Fall 2020

- **Research Activities**
  - Generate and analyze a set of realistic PNT threat scenarios
  - Develop risk mitigation strategies for Highly Automated Transportation System (HATS)
  - Craft standards and guidelines for cyber resilient PNT systems
  - Validate in real-world jammed and spoofed environments

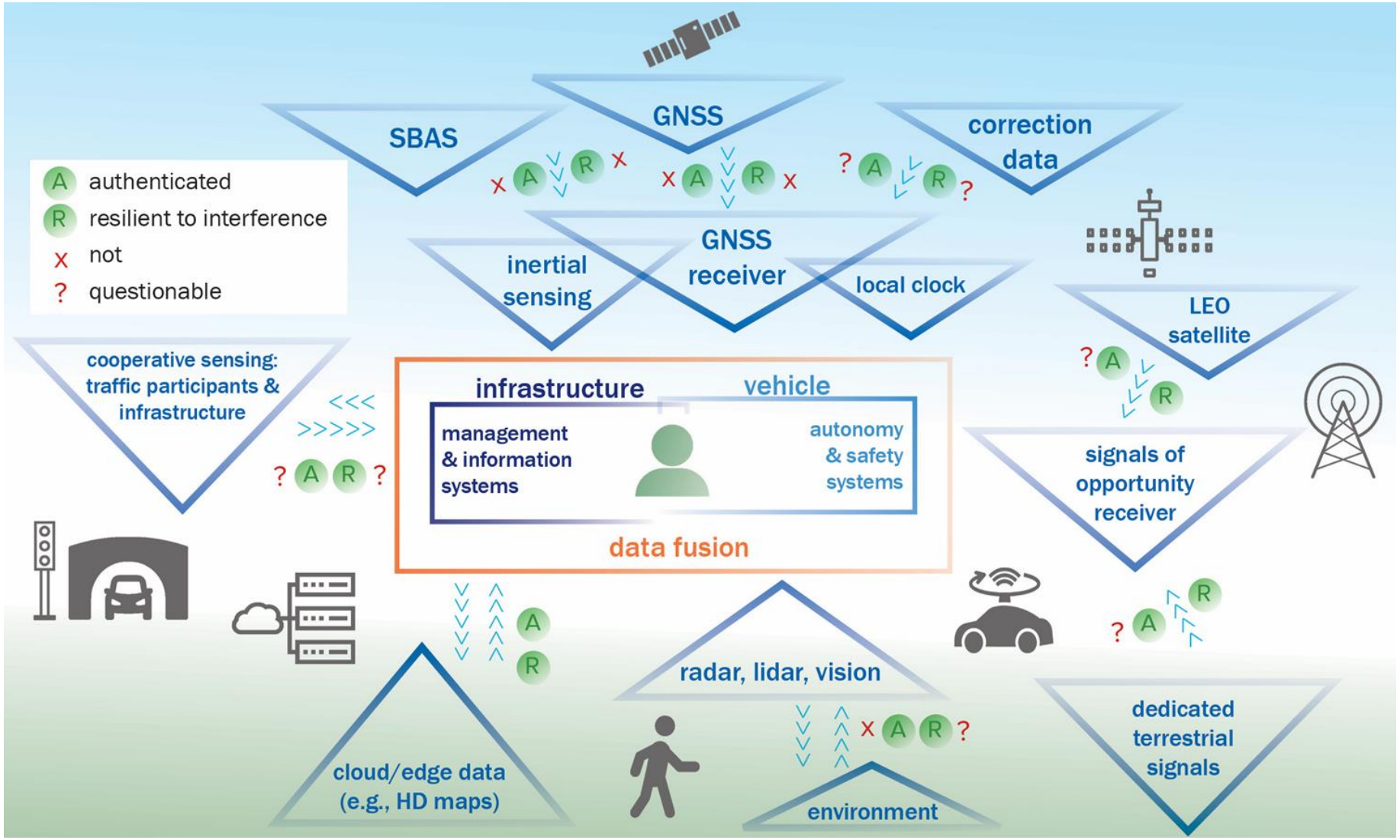
THE OHIO STATE UNIVERSITY

- **Education & Workforce Development**
  - Curricula, senior design projects, and K-12 outreach
  - Exchange program and connecting students with industry

- **Technology Transfer & Collaboration**
  - Industry Advisory Board: 35+ stakeholders
  - Bi-annual symposium

University of CINCINNATI

CARMEN University Transportation Center Vision



DOT Focus on PNT for Highly Automated Systems

PNT for Automated Vehicles (AV): ITS Joint Program Office

- AV use cases / scenarios
- Determine PNT requirements for AV operations
- Assess GNSS and other candidate sensor technologies
- Analyze PNT performance of individual sensors
- Determine navigation performance enhancements achieved by sensor fusion

DOT University Transportation Center: Highly Automated Transportation System Research

- Vulnerability cataloging and test threat vector development
- Resiliency testing
- Standards, Guidelines, and Best-practices for cyber resiliency

OST-R Highly Automated System Safety Center of Excellence

- Resilient PNT Services for Highly Automated Safety Systems

Resource Implications for DOT

Areas of Significant Increase in Level of Effort or New Responsibility:

- GNSS Performance Monitoring
- Space-Based PNT Interference Detection, Monitoring, Location, and Attribution
- GPS Signal and Data Authentication
- EO 13905 Implementation
- Implementation of Complementary PNT Demonstration Recommendations

$17M Increase Requested Through OST-R Input into FY'22 President's Budget Request (Released May 28, 2021)

Questions?