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

63rd Civil GPS Service Interface Committee (CGSIC)

September 12, 2023

Space Policy Directive 7

Key DOT Responsibilities

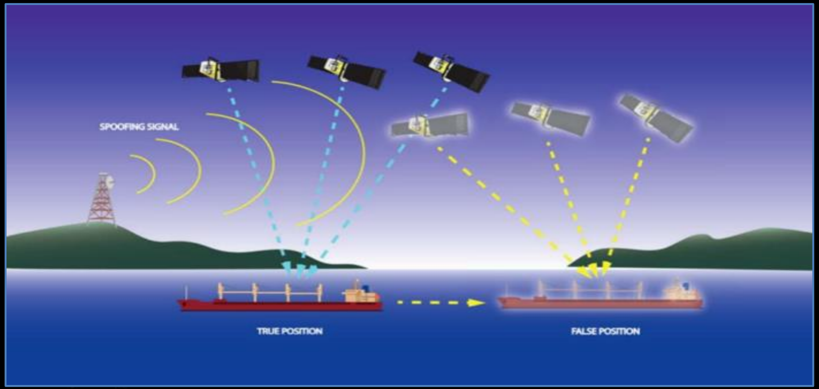
To implement SPD-7, DOT responsibilities are grouped under the following categories:

- 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

Most Recent DOT/DOD MOA on Civil Use of GPS Signed August 28, 2023

PNT Challenges for Safe and Reliable Transportation

Jamming/Spoofing/Cybersecurity



High Accuracy with Integrity

Timely
Notification of
Misleading
Information

Underground/Indoors

Urban Canyons

Reliable and Secure Connectivity

High-Definition Maps

Assured PNT: Embrace PTA Principle

- **Protect**
  - Ensure performance monitoring of space-based civil PNT services
  - Implement interference monitoring capabilities to identify, locate, and attribute PNT threats
  - Prevention of harmful interference
  - Facilitate international coordination for development of monitoring standards
- **Toughen**
  - Authenticate signals and cyber-harden user equipment
  - Utilization of CRPA Antennas
- **Augment / Adopt**
  - Implement and utilize GPS augmentations and Complementary PNT services
  - Facilitate adoption of Complementary PNT into end-user applications

US DOT PNT Research Priorities

- **GNSS Civil Signal Performance Monitoring**
  - Full Civil Monitoring Performance Specification on Civil GPS Signals (L1C, L2C, L5, and L1 C/A)
  - GPS Integrity Support Message (ISM) for Advanced Receiver Autonomous Integrity Monitoring (ARAIM)
  - Monitoring and Assessment of GNSS L-band Broadcasts
- **GNSS Interference Detection and Mitigation**
  - Monitoring, Localization, and Attribution of Interference
  - Establishing Key Government Partnerships to develop a joint automated IDM capability
  - Create a Nationwide IDM Common Operating Picture for All GNSS Stakeholders
- **GPS Signal and Data Authentication**
  - Out of Band and In Band Authentication
- **Implementation of Complementary PNT Demonstration Recommendations**
  - Facilitate Adoption of CPNT Technologies
  - Establish PNT Standards, Requirements & Conduct Vulnerability Testing and Analysis
  - Engagement with PNT Technology Vendors and Critical Infrastructure Sectors
- **EO 13905 Implementation**

DOT University Transportation Centers on PNT

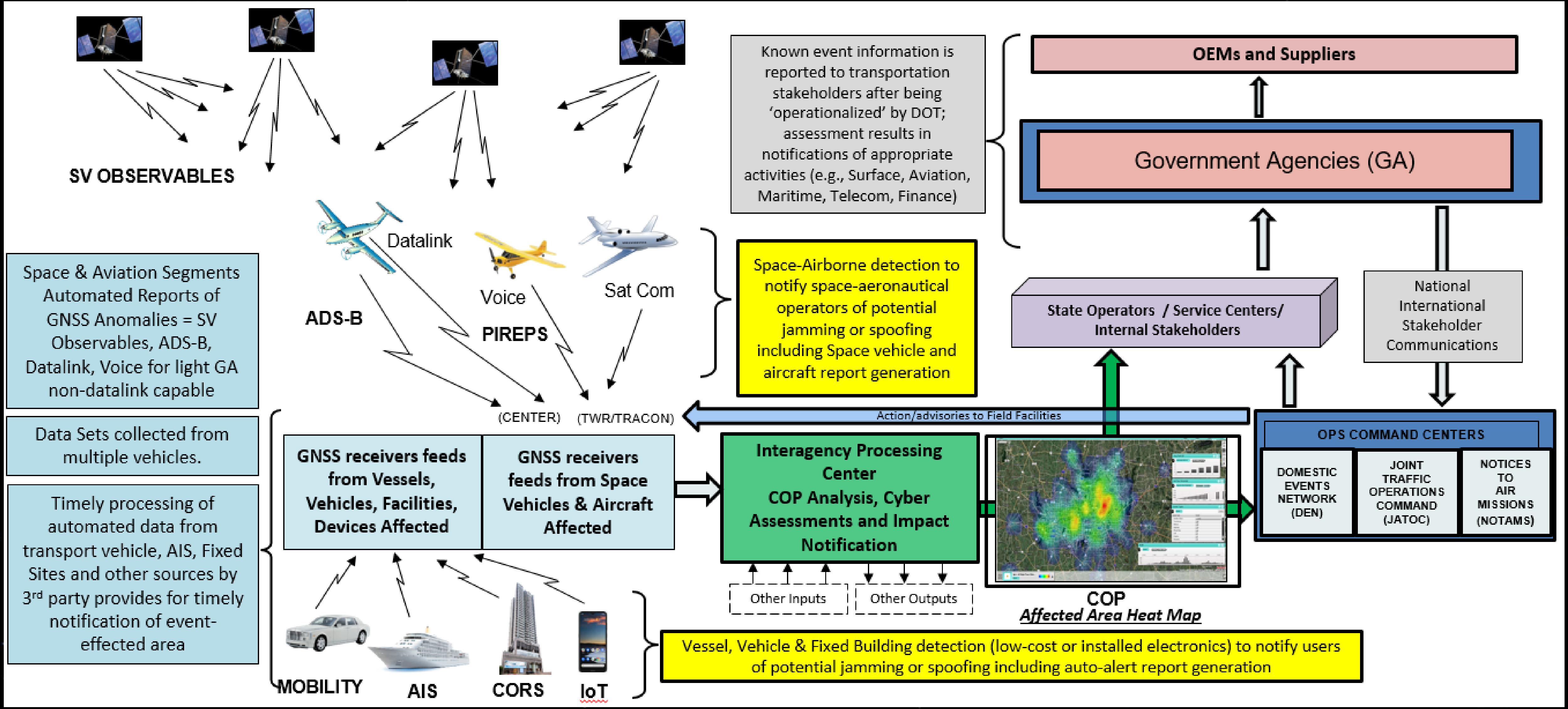
- **Center for Automated Vehicle Research with Multimodal Assured Navigation (CARMEN) - Led by The Ohio State University**
  - University Consortium Members:
    - North Carolina A&T State University
    - University of California Irvine
    - University of Texas Austin

- **Center for Assured and Resilient Navigation in Advanced Transportation Systems (CARNATIONS) - Led by the Illinois Institute of Technology**
  - University Consortium Members:
    - Chicago State University
    - Stanford University
    - University of California Riverside
    - Virginia Polytechnic Institute and State University

DOT Views on GPS/GNSS Interference Detection and Mitigation (IDM)

- PNT resiliency requires the need to detect, locate, and remove sources of interference as quickly as possible
- Relying on user reports for GPS/GNSS interference detection is extremely subjective and inadequate
- Need to have a real-time Common Operating Picture of GPS/GNSS interference based on a validated automated detection capability
    - Provide notifications and allow shared situational awareness
    - Utilize user reports of interference to corroborate automated detections
- Geolocation and direct attribution of the source of interference is critical to rapid mitigation

US DOT IDM Joint Concept of Operations



Space & Aviation Segments Automated Reports of GNSS Anomalies = SV Observables, ADS-B, Datalink, Voice for light GA non-datalink capable

Data Sets collected from multiple vehicles.

Timely processing of automated data from transport vehicle, AIS, Fixed Sites and other sources by 3rd party provides for timely notification of event-effected area

Known event information is reported to transportation stakeholders after being 'operationalized' by DOT; assessment results in notifications of appropriate activities (e.g., Surface, Aviation, Maritime, Telecom, Finance)

OEMs and Suppliers

Government Agencies (GA)

Space-Airborne detection to notify space-aeronautical operators of potential jamming or spoofing including Space vehicle and aircraft report generation

State Operators / Service Centers/ Internal Stakeholders

National International Stakeholder Communications

GNSS receivers feeds from Vessels, Vehicles, Facilities, Devices Affected

GNSS receivers feeds from Space Vehicles & Aircraft Affected

Interagency Processing Center
COP Analysis, Cyber Assessments and Impact Notification

COP
Affected Area Heat Map

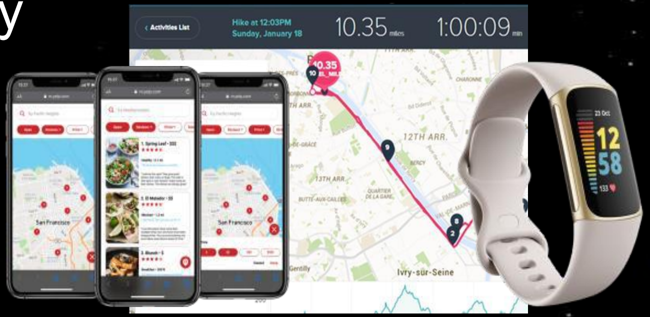
OPS COMMAND CENTERS

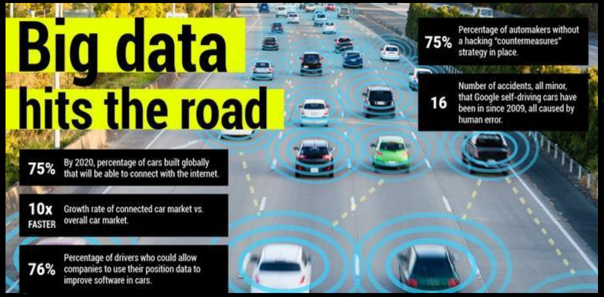
DOMESTIC EVENTS NETWORK (DEN)	JOINT TRAFFIC OPERATIONS COMMAND (JATOC)	NOTICES TO AIR MISSIONS (NOTAMS)

Vessel, Vehicle & Fixed Building detection (low-cost or installed electronics) to notify users of potential jamming or spoofing including auto-alert report generation

DIU Harmonious Rook Vision – Ideal for DOT IDM

- **Turn the Vulnerability Into a Solution:**
  - Billions of distributed, networked GNSS devices act as sensor discovery for PNT disruptions
  - Inform the use of custom, hardware centric solutions with timely classification and attribution
- **End-to-End Unclassified Workflow:**
  - Maximize discretion for sharing and dissemination with civil agencies, allies and public
- **Domain agnostic datasets:**
  - Broad coverage, classification of events, and confidence in reporting (AIS, ADS-B, IoT, SIGINT); Multi-source-Multi-Vote
- **Mixture of rule-based and ML analytics:**
  - Performance verification unsupervised clustering models
- **Actionable insight to both the analyst and the operator:**
  - Operator View: Can I expect degraded PNT on this mission?
  - Analyst View: Is there a new anomaly in my AOI?





Big data hits the road

75% Percentage of automakers without a hacking "countermeasures" strategy in place.

16 Number of accidents, all minor, that Google self-driving cars have been in since 2009, all caused by human error.

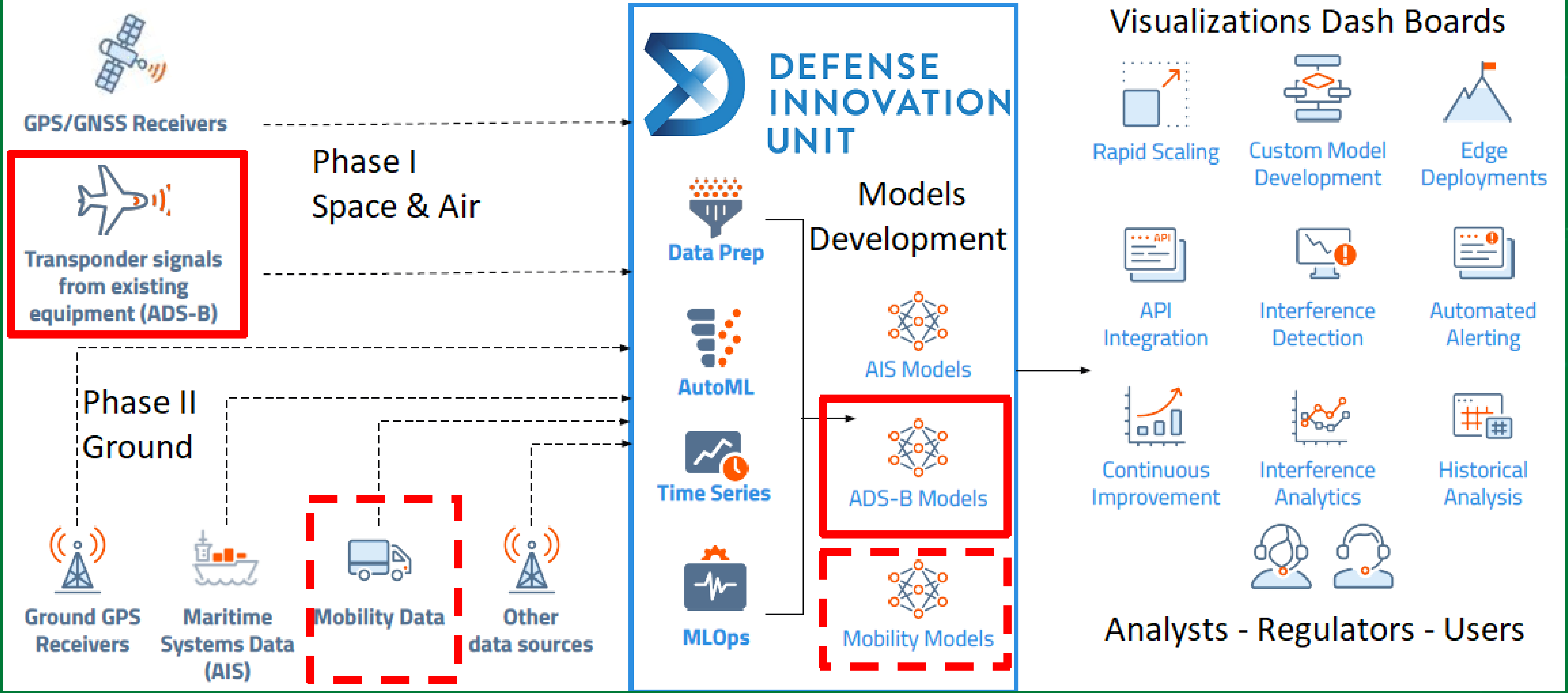
75% By 2020, percentage of cars built globally that will be able to connect with the internet.

10x FASTER Growth rate of connected car market vs. overall car market.

76% Percentage of drivers who could allow companies to use their position data to improve software in cars.

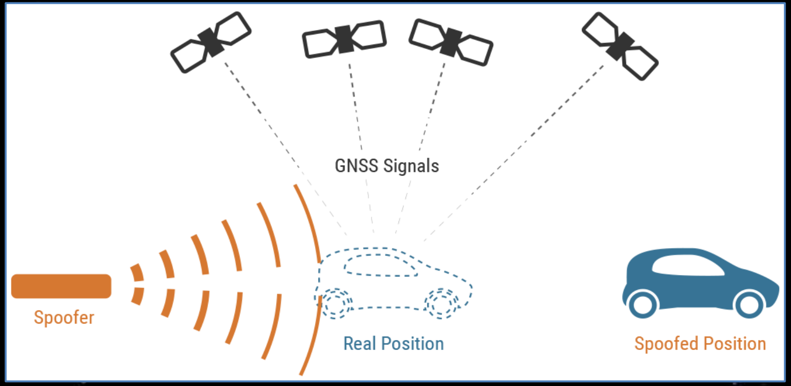
US DOT-DOD Joint Harmonious Rook IDM Initiative

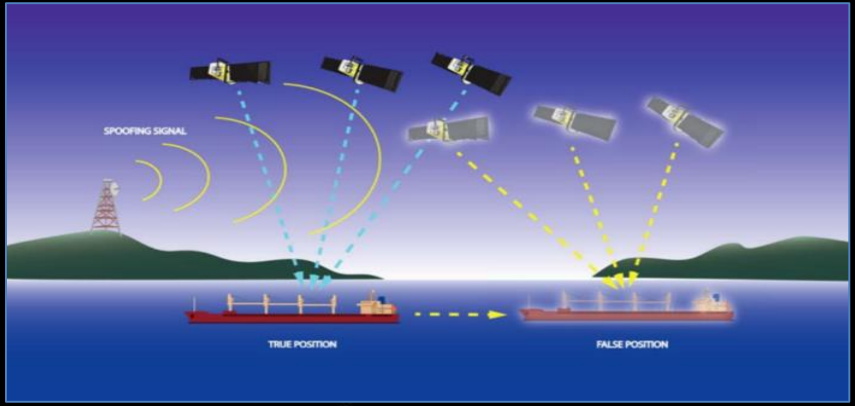
Initiating the Interagency Automated Processing Fusion Center



Executive Order 13905: Key Actions for DOT (In Conjunction with DHS)

- Vulnerability Assessment / Testing – Aviation, Maritime, Rail, Automated Vehicles
- PNT Profile Development – NISTIR 8323
- Maritime Pilot Program
- National R&D Plan on PNT Resilience
- Resilient PNT Conformance Framework Working Group
    - IEEE standards development
- Development of PNT Resilience Contract Language





“Responsible use of PNT services” means the deliberate, risk-informed use of PNT services

Complementary PNT Demonstration Recommendations

- **Safety-critical PNT requirements and standards development**

- **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

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

Focus on widespread adoption of Complementary PNT capabilities

US DOT Complementary PNT Industry Roundtable
Aug. 4, 2022

Complementary PNT vendors voiced their vision for paths forward to resilience:

- GPS has had excellent reliability and is a market anomaly created by the impression that it is a free service/utility; cost is a concern for adoption of other PNT technologies
- CPNT technologies must provide increased capability, not viewed only a backup to GPS
- “Sandbox” facilities, test ranges, and pilot programs for soft entry to mature operations
- CPNT technologies need to have a mature threat posture against capable actors
- CPNT must be viewed as a system-of-systems approach with layered/overlapping service
- Need Federal PNT contract language / USG to lead as an investor/subscriber of services
- Standards and requirements serve a role to promote innovation and adoption

Critical infrastructure owners and operators reflected views:

- USG must demonstrate commitment to resilience through procurement of these services
- Cost and technology risk are decision factors for CPNT vs. GPS in fixed infrastructure

Video from Complementary PNT Industry Roundtable

https://www.transportation.gov/pntindustryround

PNT Industry Roundtable – Bottom Line and Next Steps

Bottom Line:

- It will take a combination of the awareness of PNT vulnerabilities, use of Pilot Programs, Grants (Critical Infrastructure Sector Users), and other programs put in place to ensure the transition from experimentation to actual adoption of Complementary PNT services and products

Next Steps:

- DOT has developed an action plan that leads to adoption of CPNT capabilities
  - Participate in Resiliency Standards Bodies to Develop Stringent Performance Specifications
  - Develop PNT Performance Assessment and Vulnerability Test Ranges
  - Make the U.S. Government a Lead Adopter of Complementary PNT Services
  - Establish a Federal PNT Services Clearinghouse
  - Develop Application Domain Acquisition Support for Complementary PNT Services Procurement

CPNT Sandbox capabilities or Field Test Ranges leverage products and outcomes from the standards, vulnerability testing, and performance assessment

DOT Complementary Action Plan and RFI
September 11, 2023

Release of DOT Complementary PNT Action Plan:

https://www.transportation.gov/sites/dot.gov/files/2023-09/DOT%20Complementary%20PNT%20Action%20Plan.pdf

DOT Volpe Center Complementary PNT Sources Sought / RFI:

https://sam.gov/opp/6350a17e5b8a4419b4029b17cb2d9b3f/view

“The Volpe Center is issuing this RFI seeking information from industry about availability and interest in carrying out a small-scale deployment of very high technical readiness level (Technology Readiness Level (TRL)≥8) CPNT technologies at a field test range to characterize the capabilities and limitations of such technologies to provide PNT information that meet critical infrastructure needs when GPS service is not available and/or degraded due environmental, unintentional, and/or intentional disruptions.”

Submission Due Date: September 25, 2023

Questions?