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

National Space-Based PNT Advisory Board Meeting
December 4, 2024

Assured PNT: Embrace PTA Principles

- **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

Need for PNT Situational Awareness (SA)

- GPS/GNSS jamming and spoofing is a growing problem for DoD, DOT, and US critical infrastructure – not limited to localized threats or effects
  - Problem highlighted by U.S. Government directives, include Space Policy Directive 7 (SPD-7)
- Situational awareness provides enhanced resilience to the current and future PNT architecture through the detection, characterization, attribution, and geolocation of interference, regardless of source or intent
- DOT-DoD working to develop a coherent strategy to address threats and needs across government
  - Desire to leverage current technology and streamline investment for a dual-use capability, to include allied use and investment
  - Identify and close gaps in PNT SA capabilities

PNT SA is a critical capability to enhance the resilience of current and future PNT technologies, ensures safety and critical infrastructure functionality

Emerged GPS/GNSS Threats

- Mar 2019 Non-profit (C4ADS) exposed Russian Spoofing in Europe with over 10,000 events detected at 10 locations between 2016 and early 2019

  Low cost, commercially availability, and ease of deployment of (SDR) technologies empowers not only state entities, but insurgents, terrorists, and criminals in wide range of destabilizing state-sponsored and non-state illicit networks

  GNSS jamming and spoofing endangers everything from global navigation safety to civilian finance, logistics, and communication systems

- From 8/15 to 9/15 2024: ~ 41,000 Boeing, Airbus and other aircraft flights assessed by ADS-B as impacted by collateral spoofing effects
  - Per Zurich University of Applied Sciences designed SkAI open-source tool
- Spoofing now routine adjacent to conflict zones & near many C-UAS sites
- Additionally, commercial aircraft are experiencing time, horizontal and vertical position jamming and spoofing far from conflict zones and in all phases of flight

Components of PNT SA

Sensors – Agile Meridian, UHU, HRTR, SDA, Hawkeye 360

Receivers – DoD, Civil (space-based data, commercial aviation via ADS-B, maritime via AIS, cell phone data, etc.)

Much of this data can be leveraged from existing tools: DEEP PNT, Harmonious Rook, FAA NOPAS

Data Transport & Storage – Sensor to fusion engine; analysis (SA) to user

Leverage DoD and commercial comms for data transport and storage (e.g. AWS Cloud)

Fusion Techniques – Employ multisensor fusion techniques to rapidly process senor data and produce actionable products

Detection, characterization, and geolocations of interference sources

Display interference heat maps to display probable effects on receivers

Scalable Visualization & Analysis Tools – GNSS Operational Awareness Tool (GOAT) driven by multiple sources (e.g. Navigation Performance Augmentation System (NOPAS), Harmonious Rook, DEEP PNT, etc.)

US PNT SA Architecture is designed to be scalable to leverage multiple sensor types (regardless of owner) and use cases across diverse interagency requirements

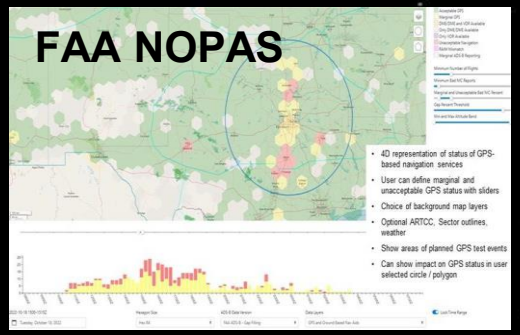
GPS Interference Detection and Mitigation

SPD-7: *"The Secretary of Transportation in coordination with the Secretary of Defense and the Secretary of Homeland Security and the heads of other agencies, as appropriate, implement Federal and facilitate State, local and commercial capabilities to **monitor, identify, locate, and attribute** space-based PNT service disruption and manipulations within the United States that adversely affect use of space-based PNT for transportation safety, homeland security, civil, commercial, and scientific purposes."*

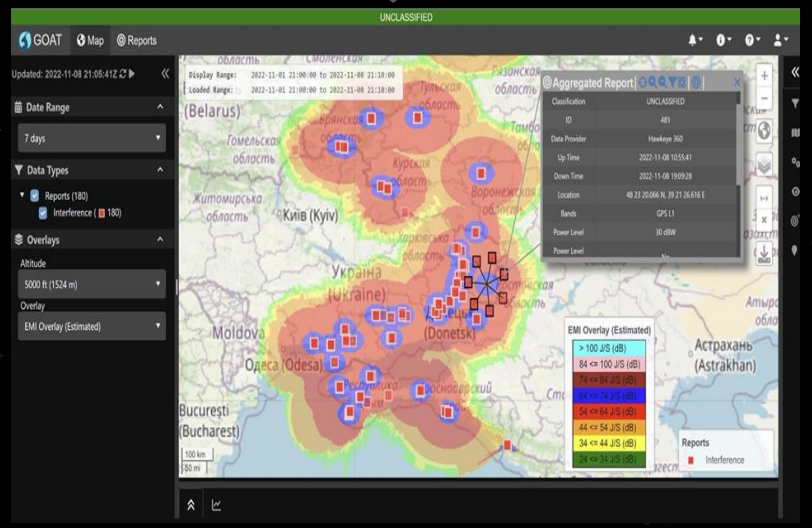
IDM Capability Need

- **Detection of EMI (Spoofing + Jamming)**
- **Geolocation for Action**
- **Mitigate/Resolve**
- **Notify in a Timely Manner**
- **Trend Analysis**
- **Awareness at User Level**

DOT-DoD Partnership: Capability for Alerting and Mitigating Threats to All GNSS Users



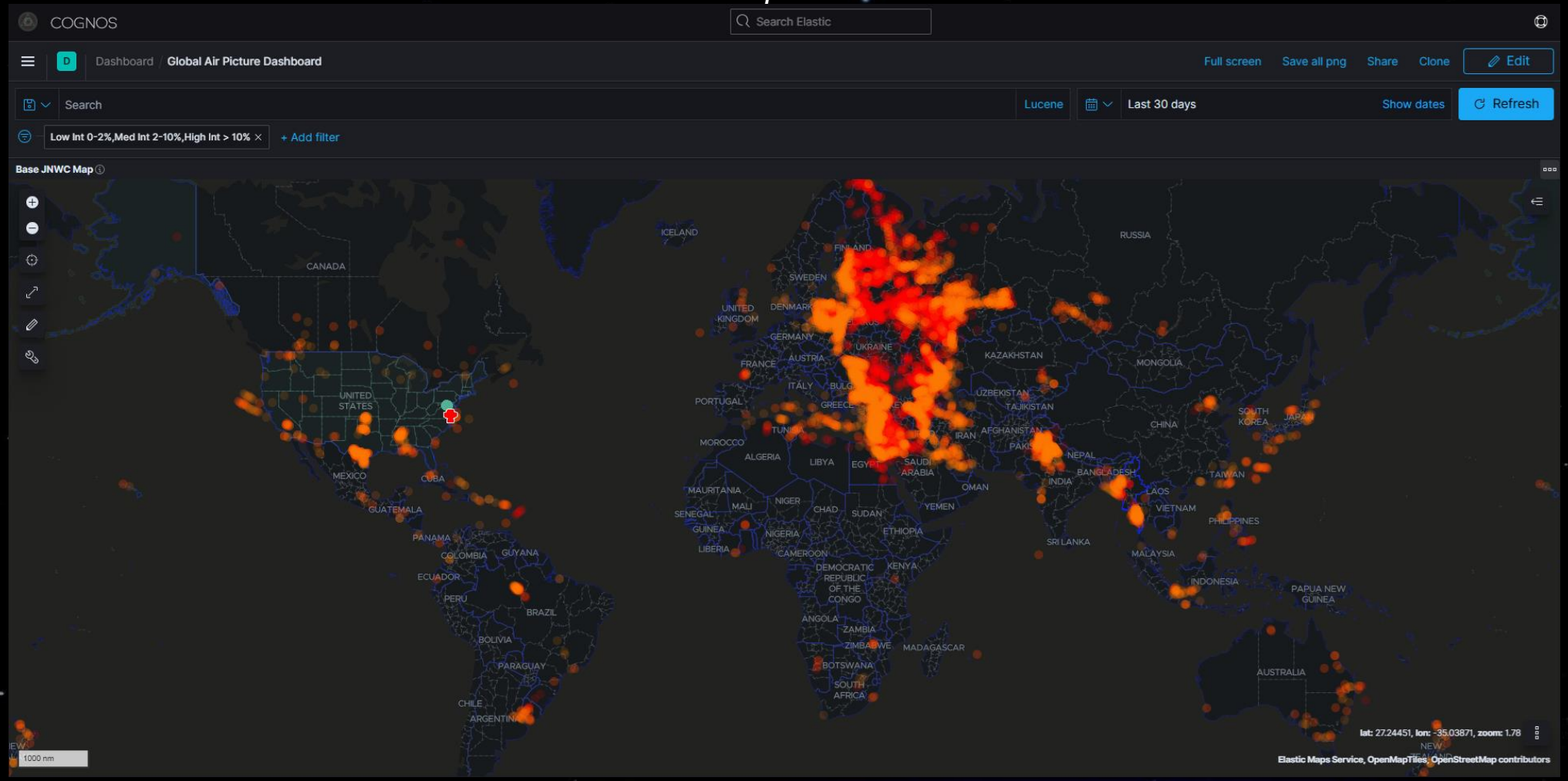
Exports anomaly detection; affected user heat maps, and estimated geolocation to GOAT GIS tool



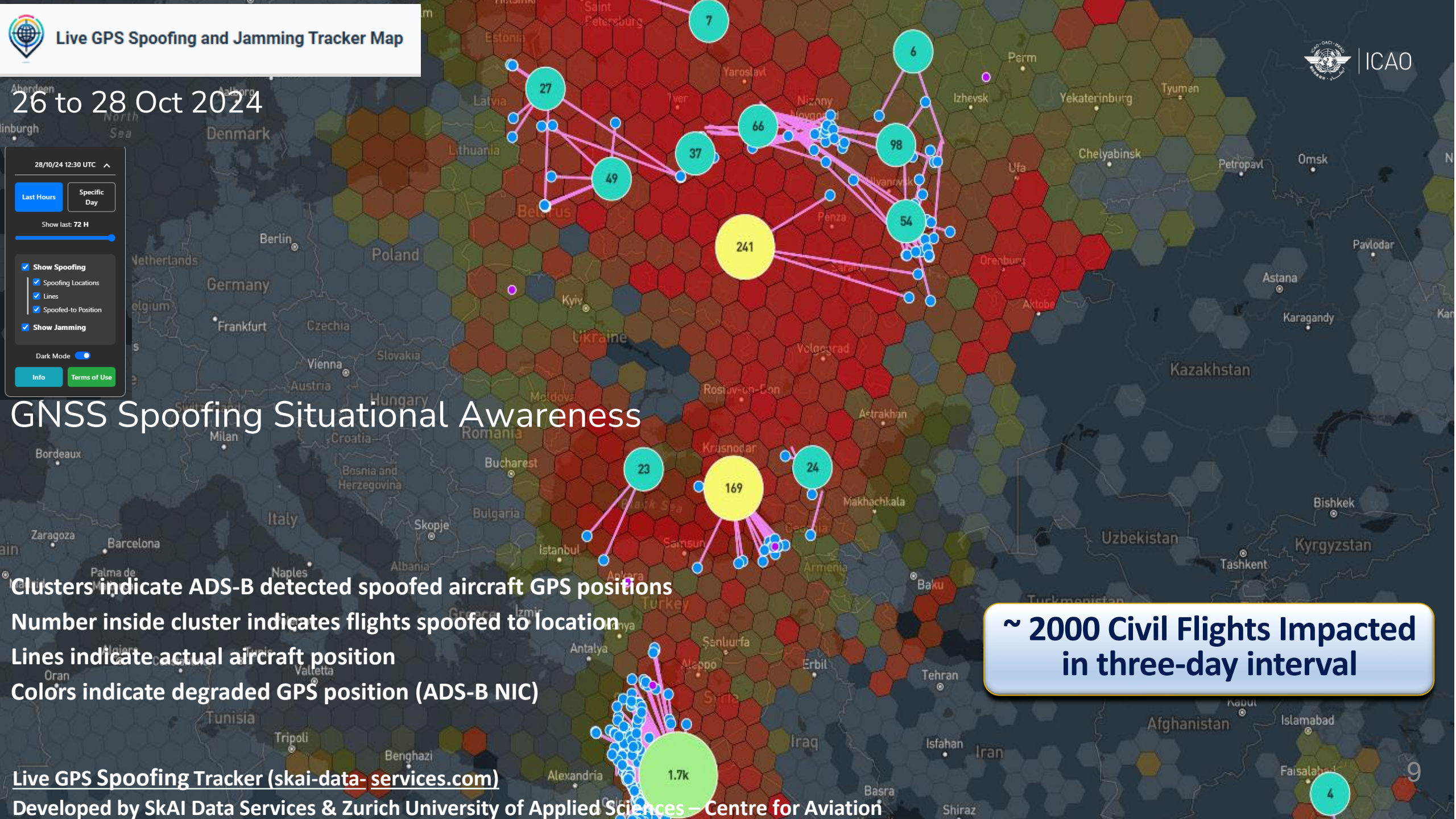
FAA is testing GNSS Spoofing Direction Finding (DF) capabilities on RFI Inspection Vehicle and plans to Research Flight Inspection Aircraft location capabilities

Development of U.S. Government GNSS IDM COP Capability

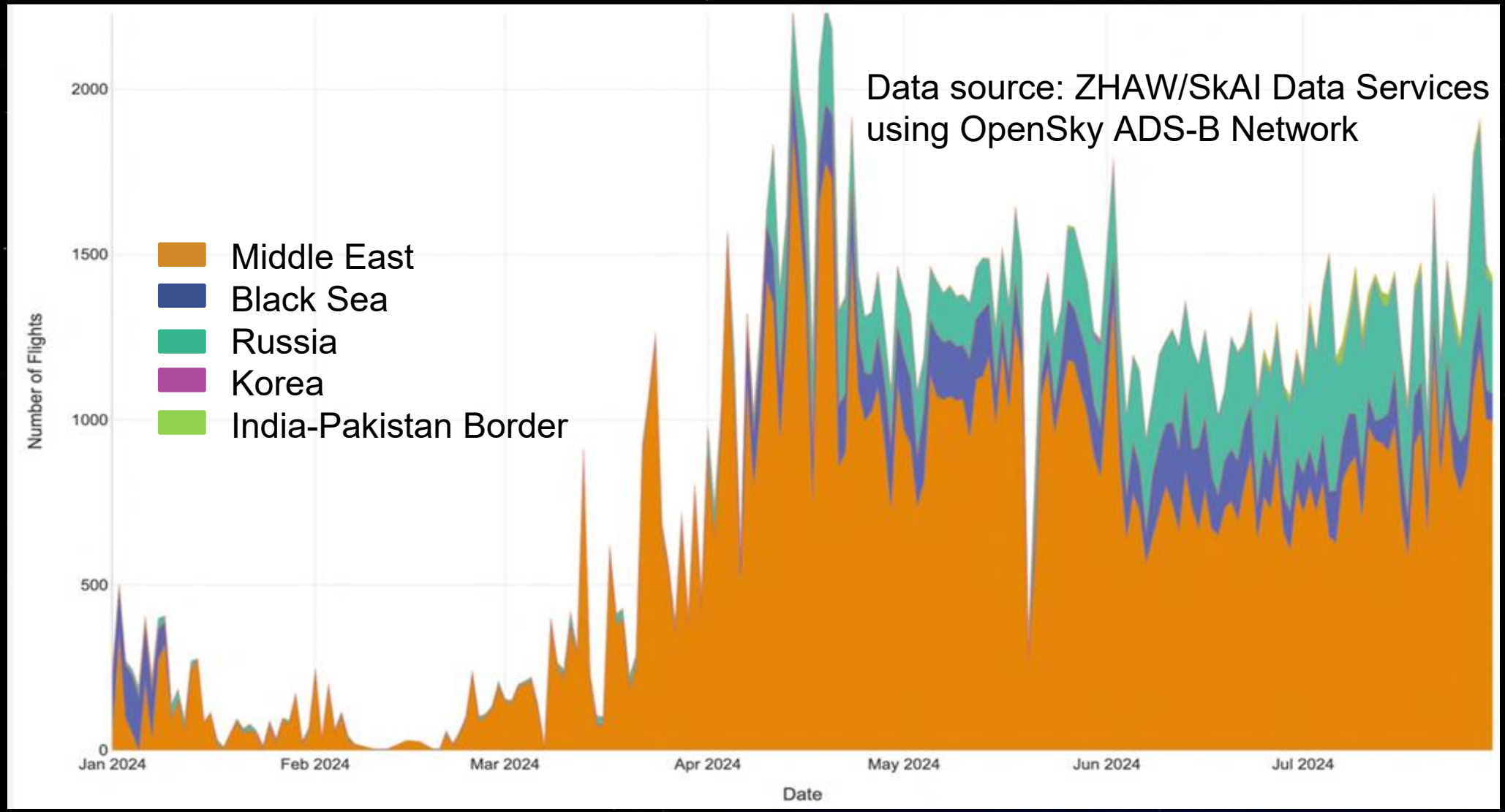
The present GNSS Situational Awareness Common Operational Picture (COP) GovCloud Environment is Operational Internally to Government Users Only at present in Three (3) Secure Environments hosted by DoD with users from DOT, DHS and other Federal Departments. User Access and Authentication Controls are Performed via ***USER CAC-PIV*** *Issued Credentials. A Public Version is planned for Middle of Calendar 2025. Enhancements and Development of Metrics in the COGNOS COP will be Included.*



New Open Source Situational Tool


Live GPS Spoofing and Jamming Tracker Map
26 to 28 Oct 2024
ICAO
28/10/24 12:30 UTC
Last Hours
Specific Day
Show last: 72 H
Show Spoofing
Spoofing Locations
Lines
Spoofed-to Position
Show Jamming
Dark Mode
Info
Terms of Use
GNSS Spoofing Situational Awareness
Clusters indicate ADS-B detected spoofed aircraft GPS positions
Number inside cluster indicates flights spoofed to location
Lines indicate actual aircraft position
Colors indicate degraded GPS position (ADS-B NIC)
~ 2000 Civil Flights Impacted in three-day interval
Live GPS Spoofing Tracker (skai-data- services.com)
Developed by SkAI Data Services & Zurich University of Applied Sciences – Centre for Aviation
7
6
27
66
98
37
49
54
241
23
169
24
1.7k
4

Estimated Number of Daily Global Flights Affected by GNSS Spoofing by Region



Numerous Commercial Situational Tools are in Development

Spoofing is A Global Threat

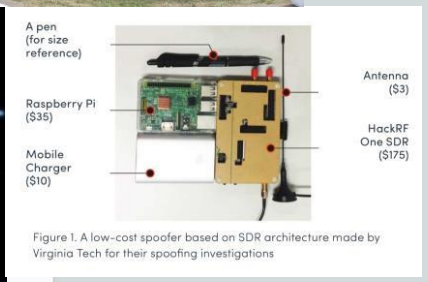
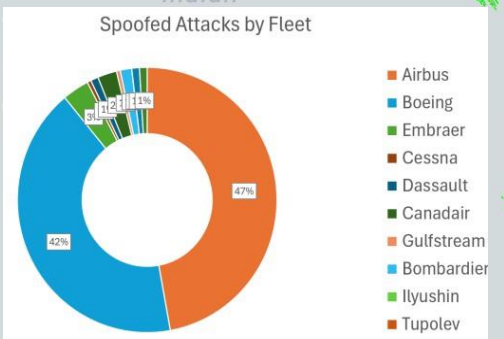


Figure 1. A low-cost spoofer based on SDR architecture made by Virginia Tech for their spoofing investigations

August 28, 2024

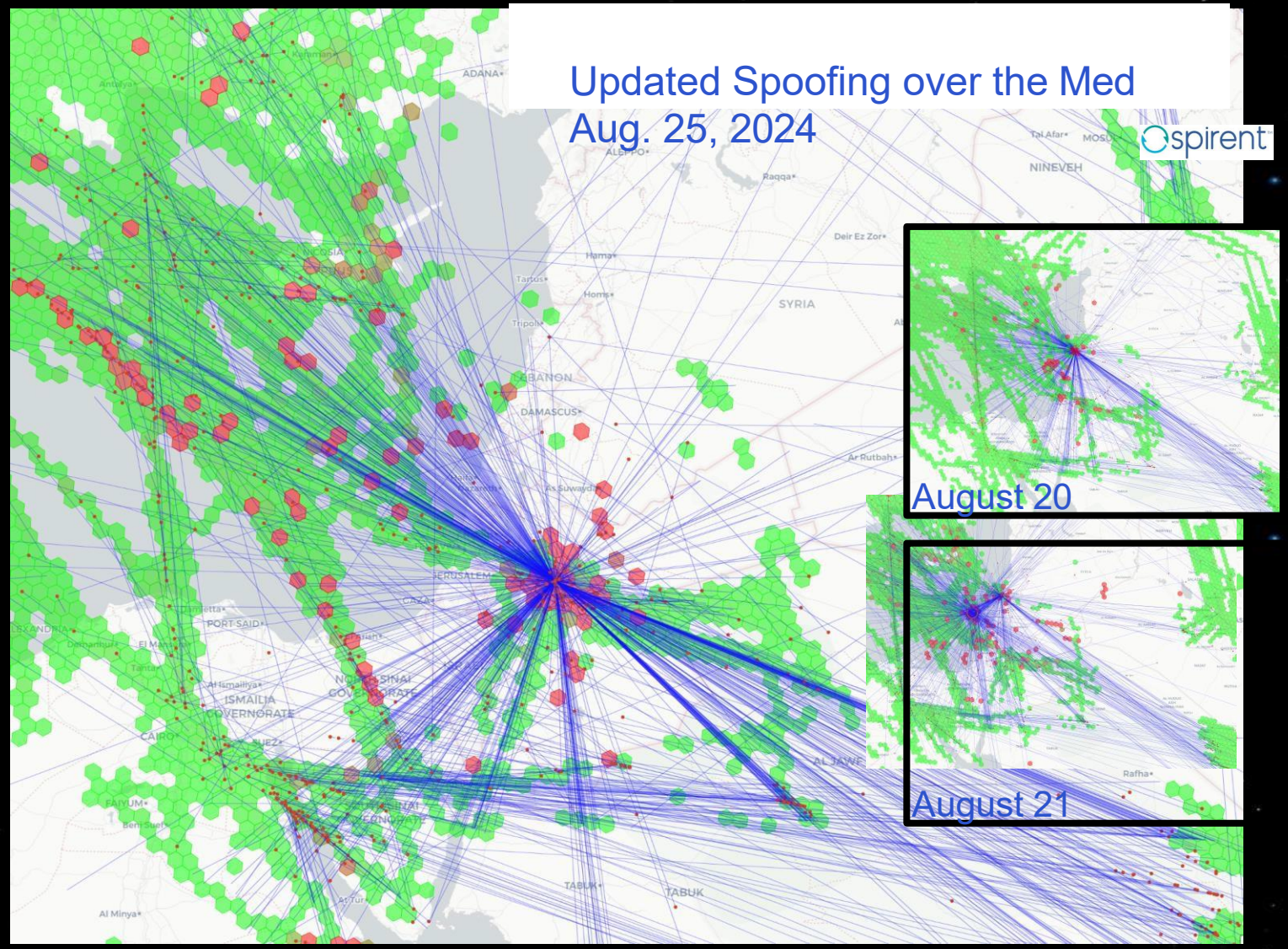


How Do You Know Where Spoofing Occurs and Impact?

- Spoofing is always changing
- Over this week we have seen:
  - Scattered signatures of Beirut & Cairo
  - Circle spoof of the coast of Israel
  - Pinpoint over OJAI in Jordan

Spoofing signature is becoming more sophisticated (not shown)

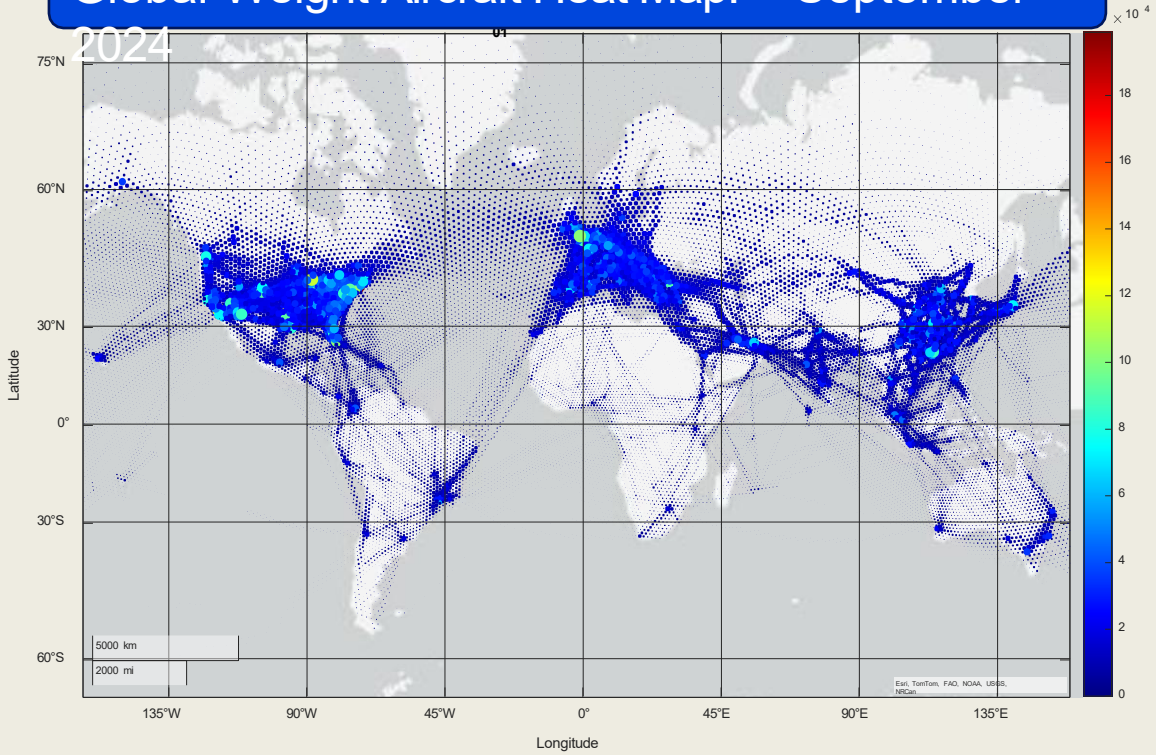
- GPS integrity varies by aircraft type and hence impact to crews & systems
- Some aircraft continue to have GPS issues after exiting the spoofed area (not shown)
- Detected in real-time service & replicated in test equipment



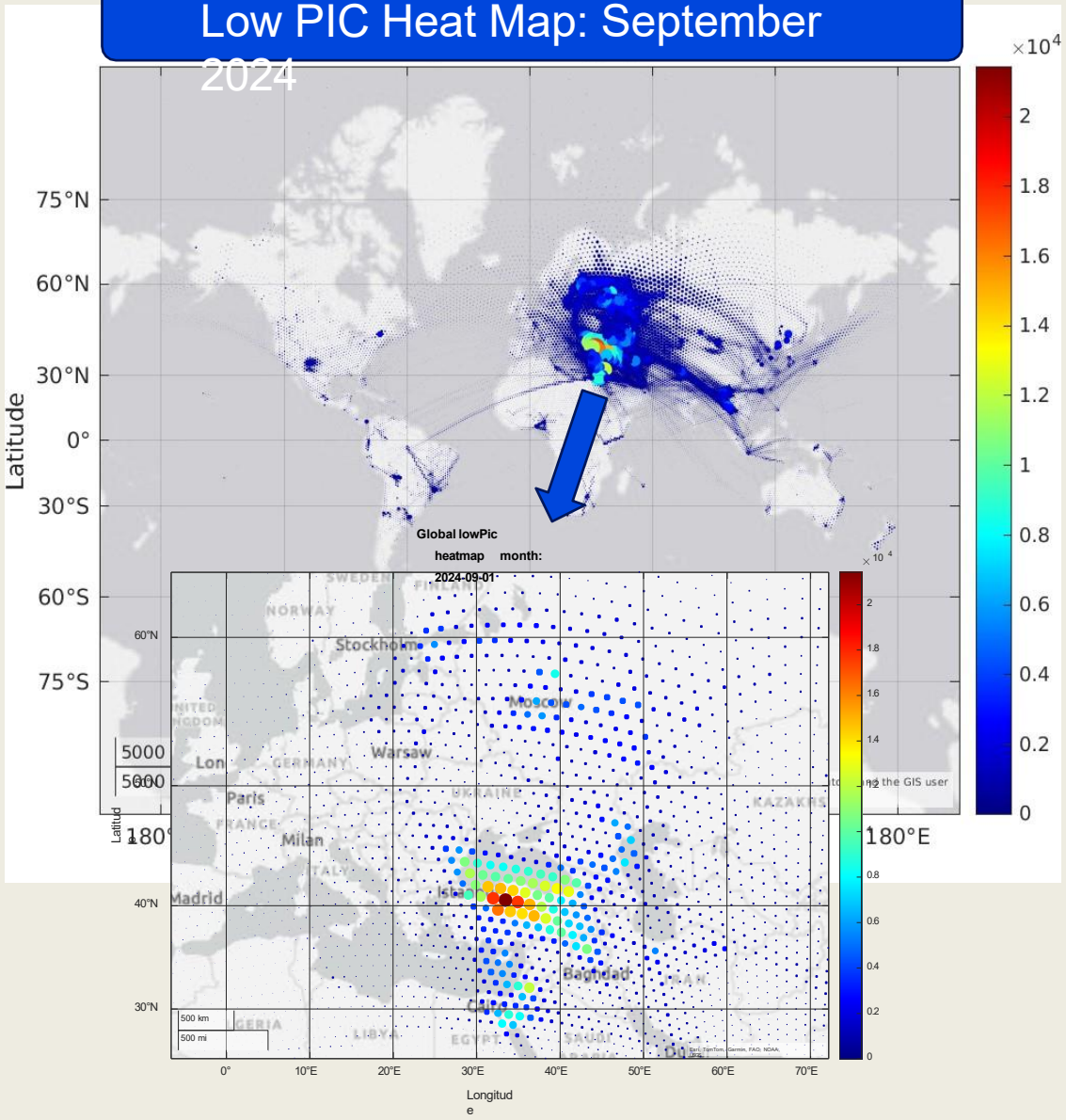
Spirent Watchman: GPS Spoofing Detection & Alerting Service

Global GNSS Interference Heat Maps: Unique to Aireon

Global Weight Aircraft Heat Map: September 2024



Low PIC Heat Map: September 2024



PIC: Position Integrity Check

Aireon

Continued Areas of Interagency IDM Collaboration

Diversity of Data Types – Testing and integration of sensors for fusion

Datasets for Decisions – Generate controlled datasets of relevant sources and scenarios for testing and comparison

Algorithm Development and Integration – Develop and test advanced algorithms for detection, precision geolocation, and effects modeling; include user-equipment-based algorithms and soft fusion techniques

Automation – Explore techniques for automated event reporting

Distribution Capability – Explore methods to “push” data to a wide-range of users across multiple comms and visualization tools

Data Formatting and Storage – Explore standardized data formats

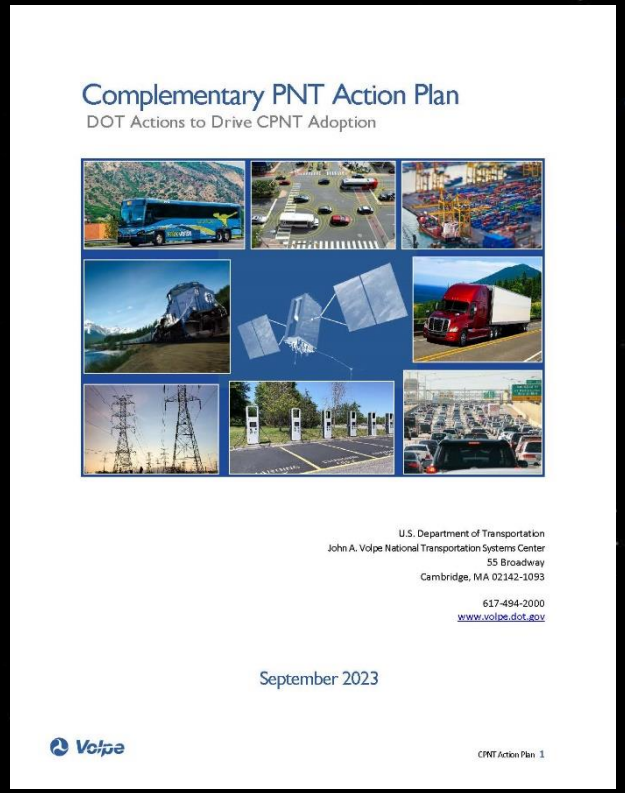
Visualization Techniques – Explore and implement “best” techniques

Multisensor Data Fusion – Explore and implement fusion techniques to enhance geolocation

DOT Complementary Action Plan, RFI, and Solicitation

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 Issued:

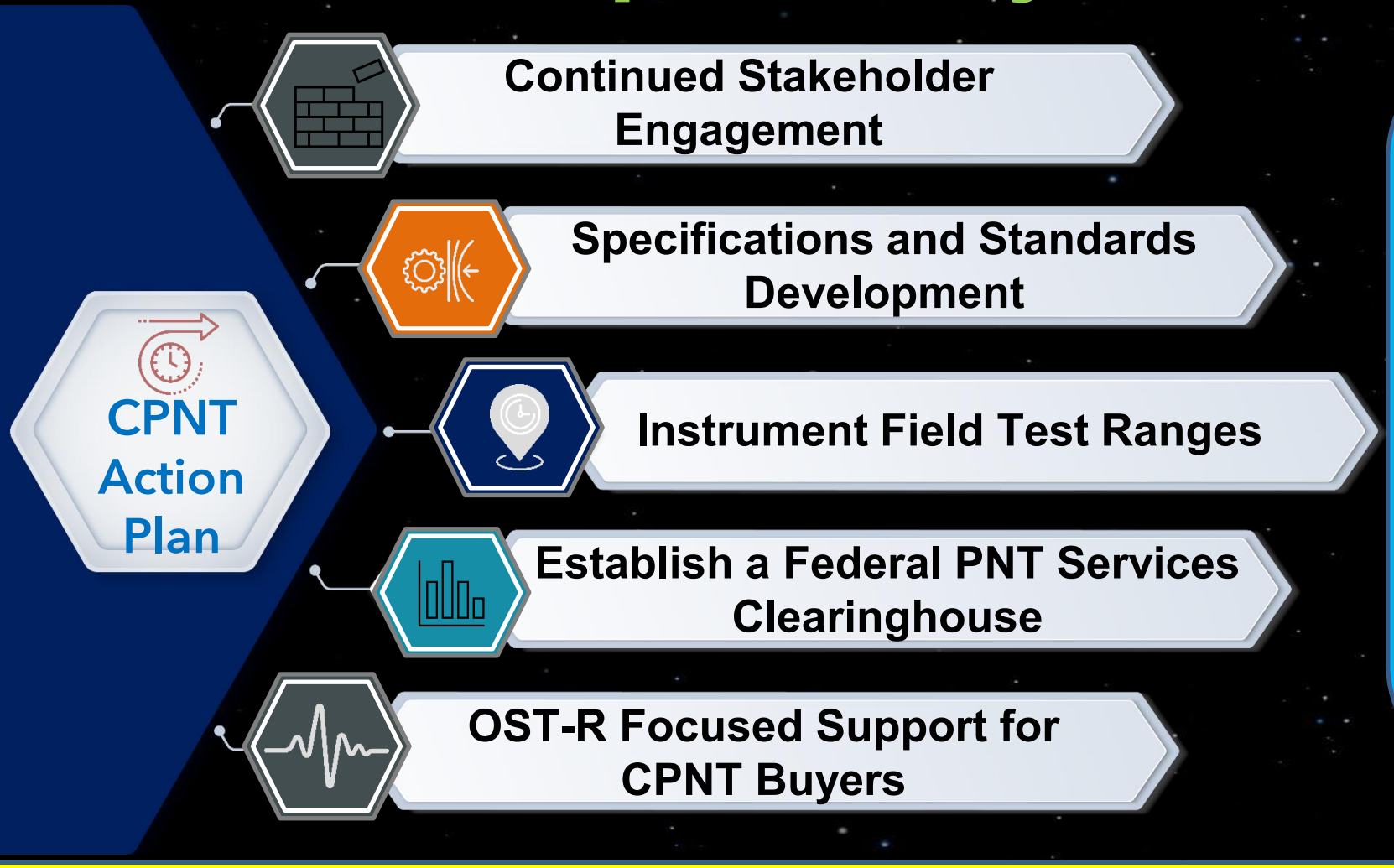
https://sam.gov/opp/6350a17e5b8a4419b4029b17cb2d9b3f/view

"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."

DOT/Volpe Center Complementary PNT Solicitation

https://sam.gov/opp/5d3764f0f0794a57b83c257d4caf2248/view

DOT Complementary PNT Action Plan



Rapid: initial phase, conduct field trials (user needs and threat vectors)

Continuity: second phase, leverage broader range of field trial platforms (also lessons learned)

Gap fill: Overlapping phase, address challenging applications

- **Expansion of DOT scope to service provisioning discovery to technology development, implementation, and service provisioning.**
- **Drive CPNT adoption across the Nation's transportation system and within other CI sectors**

DOT Complementary PNT Proposals Selected

Technology Readiness Level ≥ 8; Instrumented Within 6 Months

Num	*Name*	*Assessed TRL*	*Test Range*	*Deployment (Months)*	*Technology*	*PNT Service*	*Test Range Location*	*Partnerships*	*Cost Base Year*
1	Hoptroff Inc.	9	1	3	Fiber/Timing Distribution (10 PTP timing sources (8 NIST, 1 GNSS, 1 boundary clock))	T	JBCC (connections in NJ)	None	$934,076
2	NAL Research Corp.	9	1	4	Low Earth Orbit (LEO) (L-Band; Iridium/STL signal)	P,N,T	JBCC	STL	$144,599
3	Locata	9	1,2,3	5	2.4 GHz Industry, Scientific, and Medical (ISM) Band – Code Division Multiple Access (CDMA) signal	P,N,T	WSMR, Port of LA, and JBCC	USAF	$778,630
4	Parsons	8	1	1	LEO (S-Band; Globalstar signal)	P,N,T	JBCC	NAB	$132,416
5	Carahsoft	8	1,2	2	Camera/map matching	P,N	JBCC & Airborne Test	None	$1,556,247
6	SAFRAN	8	1	4	Fiber/Timing Distribution (White Rabbit Time-Freq. distribution, internal Rubidium clock)	T	Northeast, JBCC	None	$245,300
7	NextNav	8	3	4	Dedicated: Multilateration and Location Monitoring Service (M-LMS) band only (919.75 MHz – 927.75 MHz) Hybrid: M-LMS band + LTE/5G	P,N,T	San Francisco Bay area	Establishing a partnership with an Advanced Air Mobility company	$1,876,968
8	Microchip	8	1	6	Fiber/Timing Distribution (virtual Primary Reference Time Clock (vPRTC) Timing Services, internal Cesium clock)	T	JBCC	NIST, ORNL	$1,498,492
9	TERN AI	8	1	6	On-board Diagnostic 2 (OBD2) sensor/map tracking	P,N	JBCC	IBM Watson X and FedEx	$51,780
								Total	***$7,218,508***

Field Test Range descriptions:
(1)Federal Government-hosted
(2)Critical Infrastructure (CI)
(3)Vendor fielded

- **Kickoff Meetings with Vendors Held**
- **Site Visits Conducted**
- **Significant Effort on Test Planning**

DOT Complementary PNT Test Range Strategy

Federal test ranges: Initial site to be located on Joint Base Cape Cod (JBCC), one of the two test ranges used for the 2020 DOT CPNT Demonstration

Critical infrastructure test ranges: Test ranges that have a government affiliation (including Federal, State, and local) either through partnerships or contractual relationships

Commercial/vendor-provided test ranges: Test ranges will be used when the other two models are not appropriate and/or beneficial

- CPNT technologies require costly installations requiring numerous transmitters over large areas
- Vendors already have built operational installations, and it may be more cost effective and time efficient to utilize these existing test ranges

DOT Complementary Rapid Phase II Solicitation

- Goal is to expand set of diverse CPNT technologies
- Greater diversity of test ranges from the initial Rapid Phase beyond JBCC
- Emphasis on Critical Infrastructure partnerships
- Solicitation Issued November 27, 2024 with Proposals Due January 14, 2025

https://sam.gov/opp/396f1f1e901a4155ace2263e3c70a588/view

Thank You to the Contributors to This Briefing

DoD

John Skudlarek
Dr. Sonya McMullen
Dr. Keith McDonald (MITRE)

FAA

Ken Alexander
James Aviles
Sean Memmen

DOT/Volpe

Anne Gates
Stephen Mackey

Questions?