
NEXTNAV
The Need for Next Generation GPS

Gillian Smith

Chief Marketing Officer, NextNav

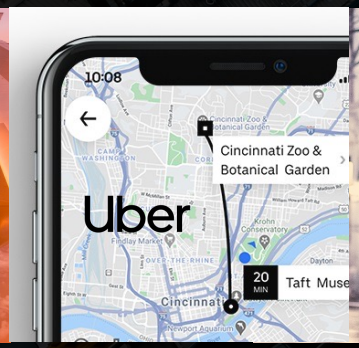
gsmith@nextnav.com

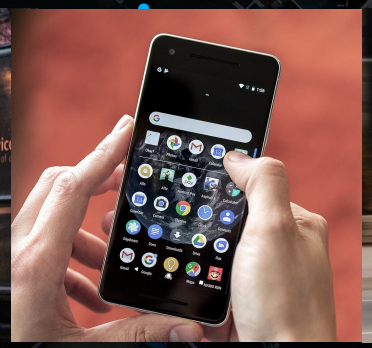
The economic benefit of GPS in the United States has been estimated at more than $1.4 Trillion USD.

GPS/GNSS provides position, navigation, and timing (PNT) services. We rely on it for aviation, agriculture, telecommunications, power grids, financial transactions, maps and more.

But, as a space-based service, GPS is vulnerable to spoofing and jamming by rogue actors and state actors, as well as natural phenomena like solar flares, and signals are unreliable in urban areas.

It is single point of failure – with no resiliency.



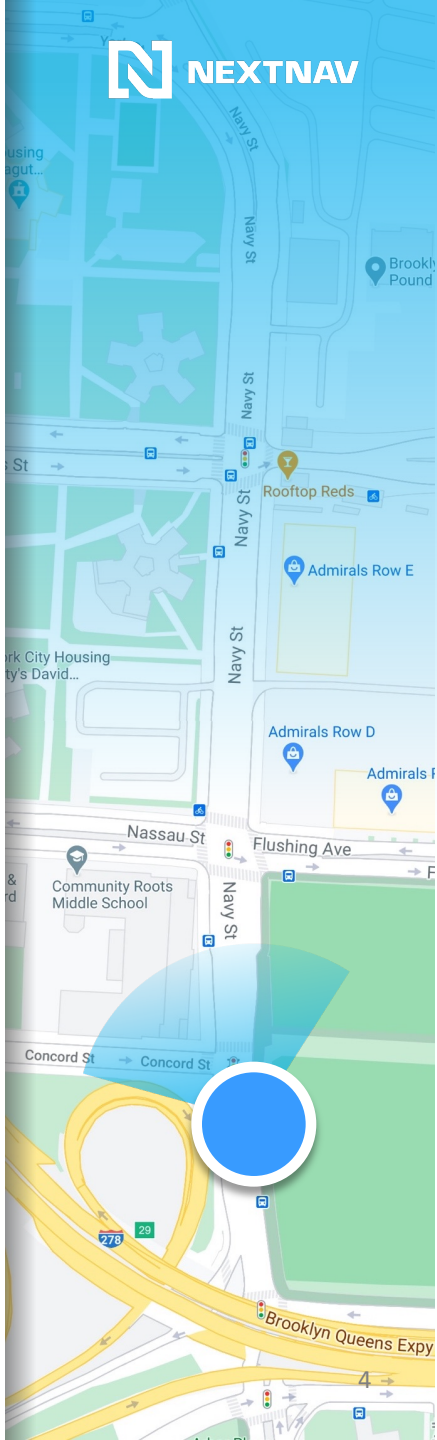


Source NIST

Industry needs have evolved beyond tech created in the 60’s

We need

- Increased accuracy and availability in urban environments
- Indoor tracking and mapping
- Altitude data (3D location)
- Increased resilience and redundancy
- Increased security

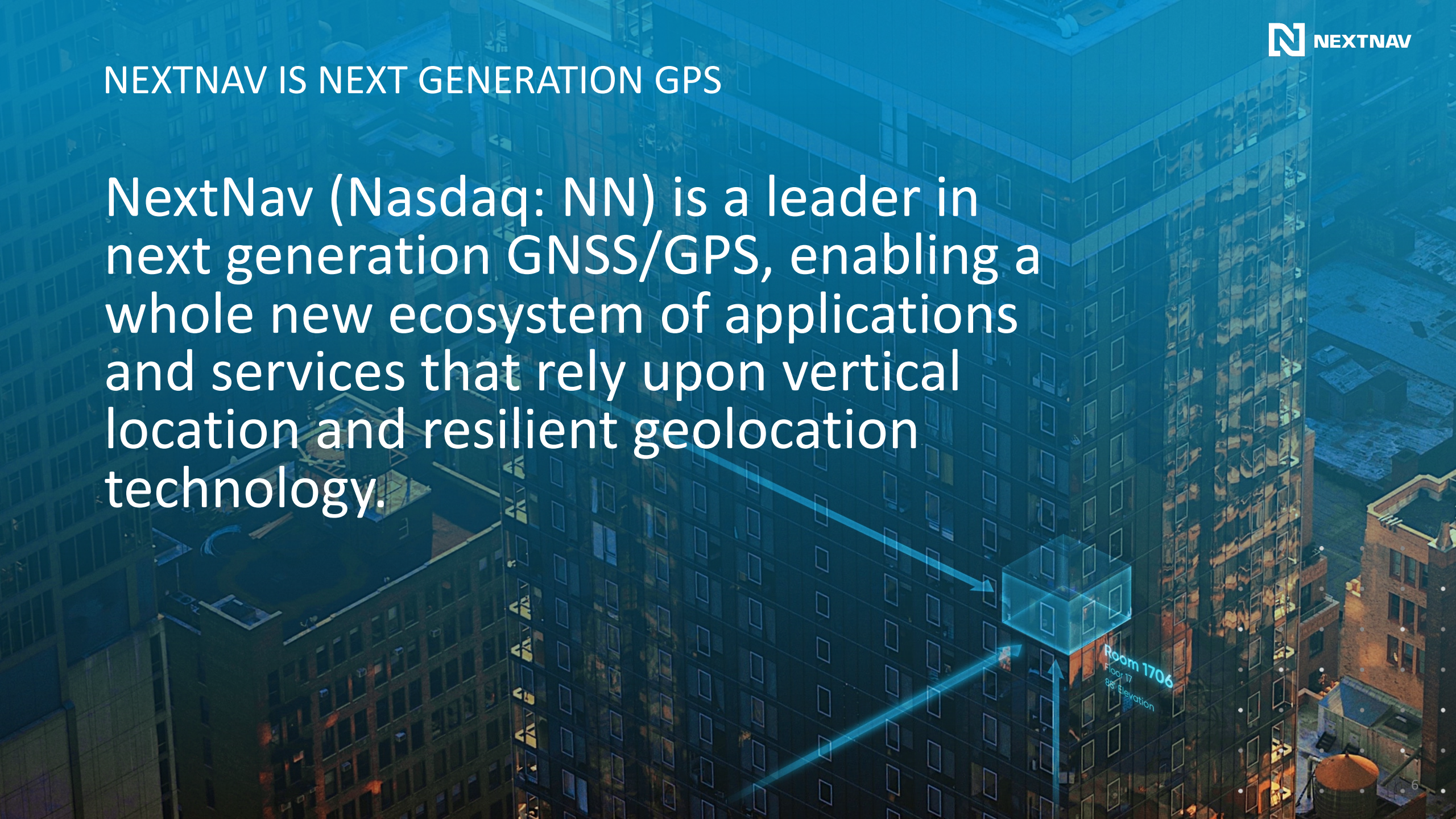


Examples of GNSS Interference

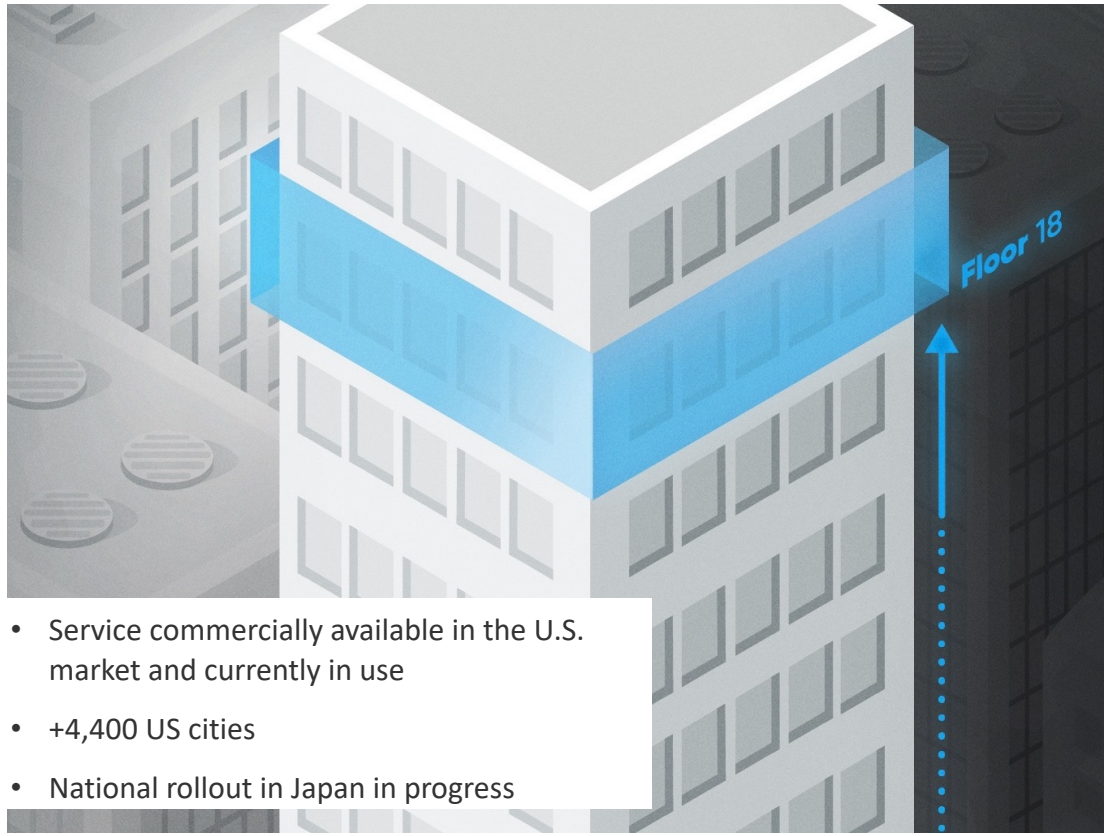
- **November 2021:** Russia shot down its own satellite and announced on state television that they could take out all of the GPS satellites used by NATO as a warning not to interfere with Ukraine
- **March 17, 2022:** EU's Aviation Safety Agency warns of GNSS spoofing and jamming in aircrafts with noted incidents in flights over Europe
- **October 2022:** the Dallas area had GPS interference for more than 36 hours, impacting air travel
- **December 2022:** Russian hacking group Fancy Bear found to have infiltrated US satellites
- **March 2023**: Qantas warns of GPS jamming from Chinese military ships in the Pacific, impacting aircrafts
- **March 2023**: One of the fastest CMEs ever recorded from the sun (Carrington-level); highest solar activity so far in 10 years

NEXTNAV IS NEXT GENERATION GPS

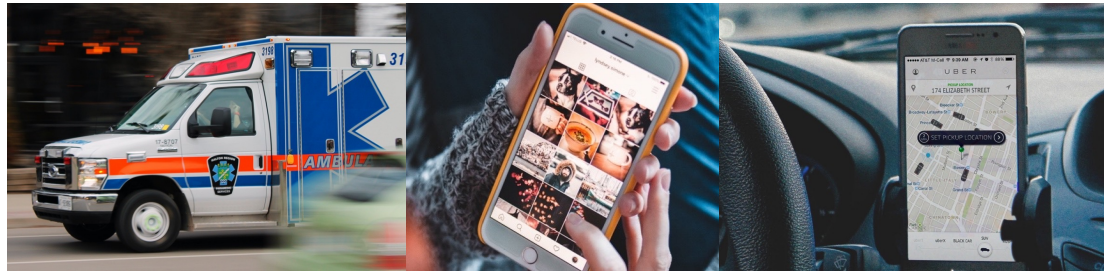
NextNav (Nasdaq: NN) is a leader in next generation GNSS/GPS, enabling a whole new ecosystem of applications and services that rely upon vertical location and resilient geolocation technology.



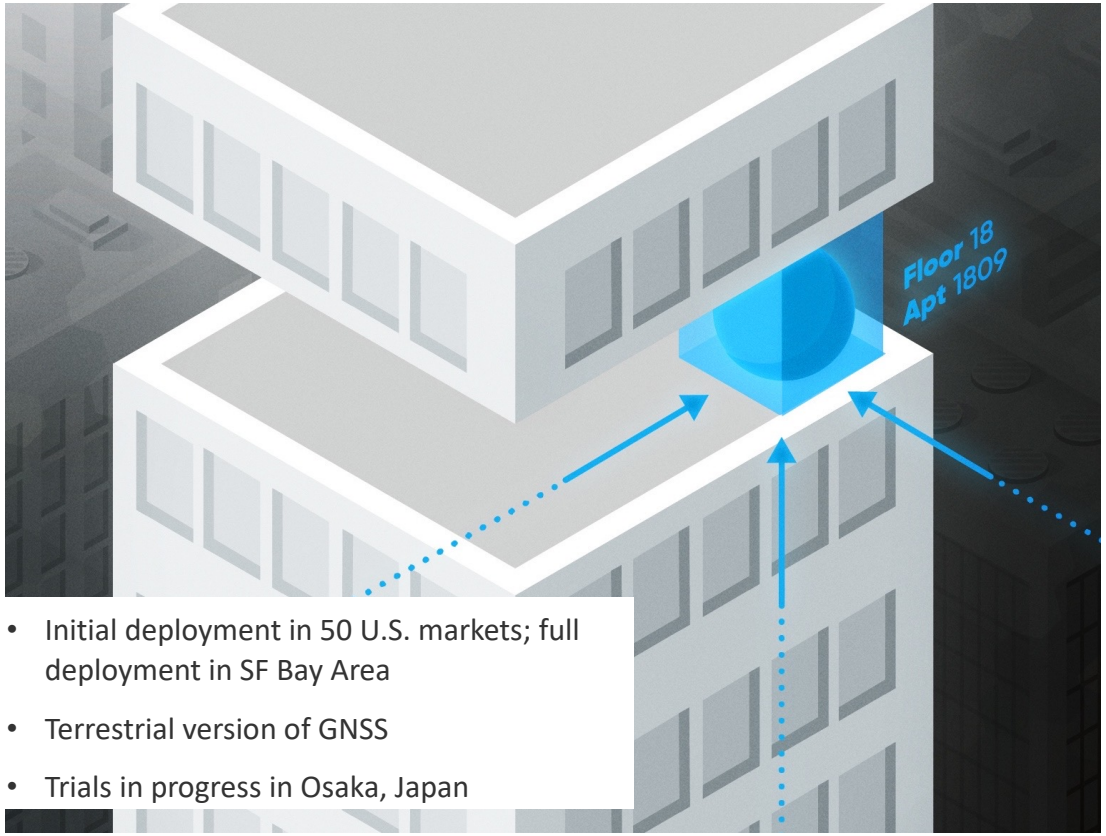
Pinnacle



- Service commercially available in the U.S. market and currently in use
- +4,400 US cities
- National rollout in Japan in progress

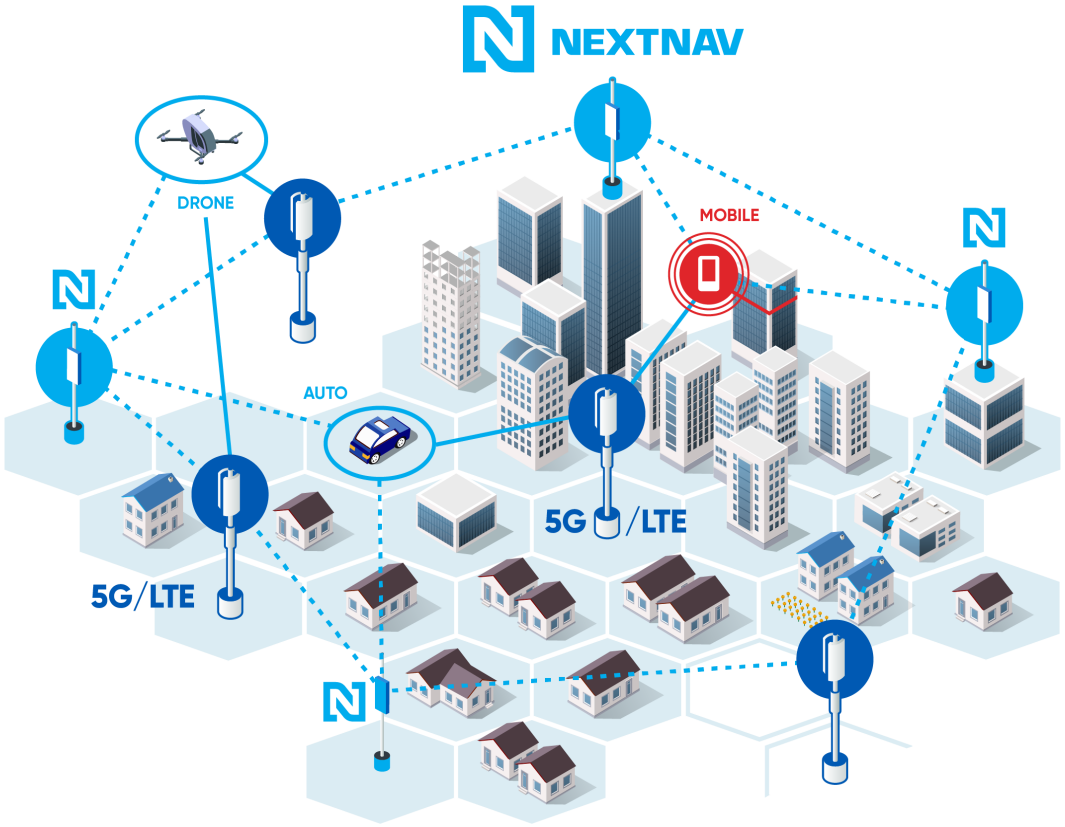


TerraPoiNT



- Initial deployment in 50 U.S. markets; full deployment in SF Bay Area
- Terrestrial version of GNSS
- Trials in progress in Osaka, Japan

TerraPoiNT – ‘Terrestrial GPS’



- ✓ Ground-based solution that provides full Position, Navigation and Timing (PNT) Capabilities – GNSS equivalent service
- ✓ Scalable – Terrestrial beacons deployed around a city and provides PNT services under its entire coverage footprint
- ✓ Ability to combine signals with existing LTE/5G networks with our own highly synchronized TerraPoiNT system for efficient deployment
- ✓ Resistant to spoofing and jamming
  - ✓ Over 100,000x stronger than GNSS signals & terrestrial in nature
  - ✓ Ability to authenticate signal (e.g., encryption)
- ✓ Can operate independent of GPS using built-in atomic clocks and ability to self-synchronize
- ✓ Relatively frequency flexible: ~ 920 MHz US, ~ 860 MHz Japan (5 MHz broadcast spectrum)
- ✓ In use by NASA with a dedicated campus in Langley for drone and urban air mobility testing, and in Mountain View, CA leveraging our deployed network
- ✓ **Tested by the US DOT and DHS: ranked #1 across all metrics for positioning, navigation and timing**

NEXTNAV

Lessons From The Field

PNT Vulnerabilities are Cybersecurity Risks

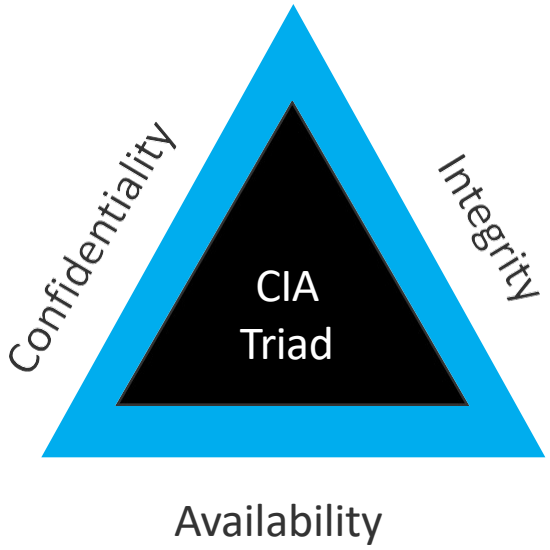
Government Needs to Create Incentives for Private Sector

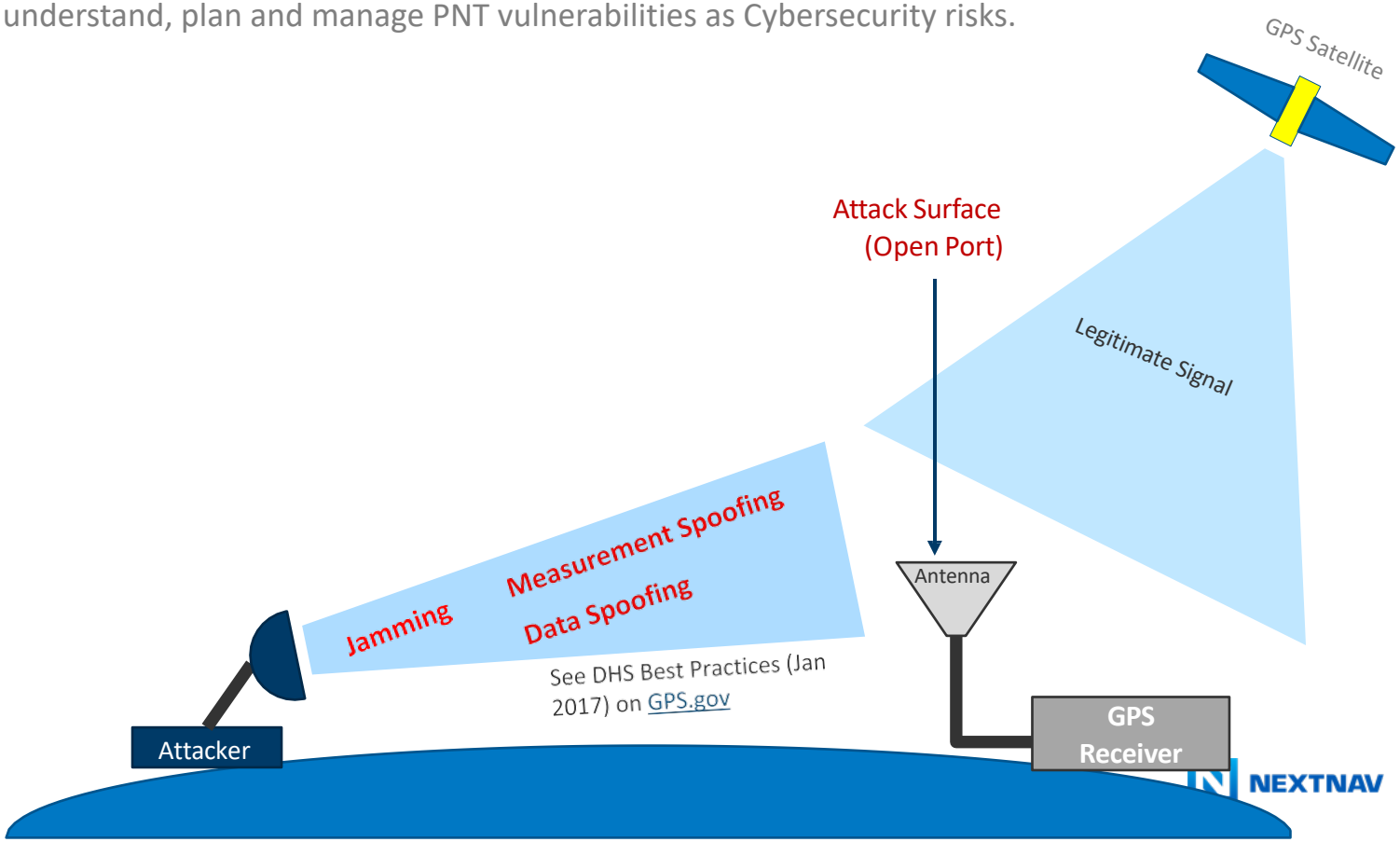
Government Needs to be First Customer

Multiple Solutions are required for PNT Resiliency

The NIST Cybersecurity Framework Refers to PNT Vulnerabilities as Cybersecurity Threats

As part of the NIST Cybersecurity Framework (CSF 2.0) & NIST PNT Profile (NIST IR 8323), PNT vulnerabilities are cybersecurity threats. Since the PNT vulnerabilities are closely tied and dependent on Cybersecurity risks (Denial of Service and Man in the Middle types of attacks), it's critical for Cybersecurity leaders to understand, plan and manage PNT vulnerabilities as Cybersecurity risks.





Science and Technology

From the DHS publication: A Cybersecurity Perspective to Addressing PNT Vulnerabilities, September 2022

GPS Vulnerabilities Are Cybersecurity Risks

Modern day GPS & PNT Solutions are more and more based on computer systems, and traditional jamming and spoofing concerns are now closely tied with cybersecurity vulnerabilities and threats. These can cause significant mal operation of critical infrastructure.

- As highlighted in the August 2022 CISA report on Time Guidance, examples of faulty timing adversely impacted NYC traffic lights in 2019 for 11 days. Interference impacts could be far-reaching, including power grids and utilities, emergency response, financial transactions, airports, and even cybersecurity investigations.
- PNT threats may include natural, manufactured, intentional, and unintentional disruptions and manipulations of components or networks, such as radio frequency interference (RFI), jamming, spoofing and cybersecurity attacks such as “Denial of Service” & “Man in the Middle (MitM)”.

GPS Threat Example	Cybersecurity Equivalent	Effect (CIA Triad)
GPS Jamming	Denial-of-Service Attack	Loss of Availability (Transient) Recovers after removal of threat
GPS Data Spoofing	Ransomware / Wiper	Loss of Availability (Persistent) Persists after removal of threat
GPS Measurement Spoofing	Data Manipulation (MITRE ATT&CK Framework T1565)	Loss of Integrity

Cybersecurity informed approach helps with identifying and managing:

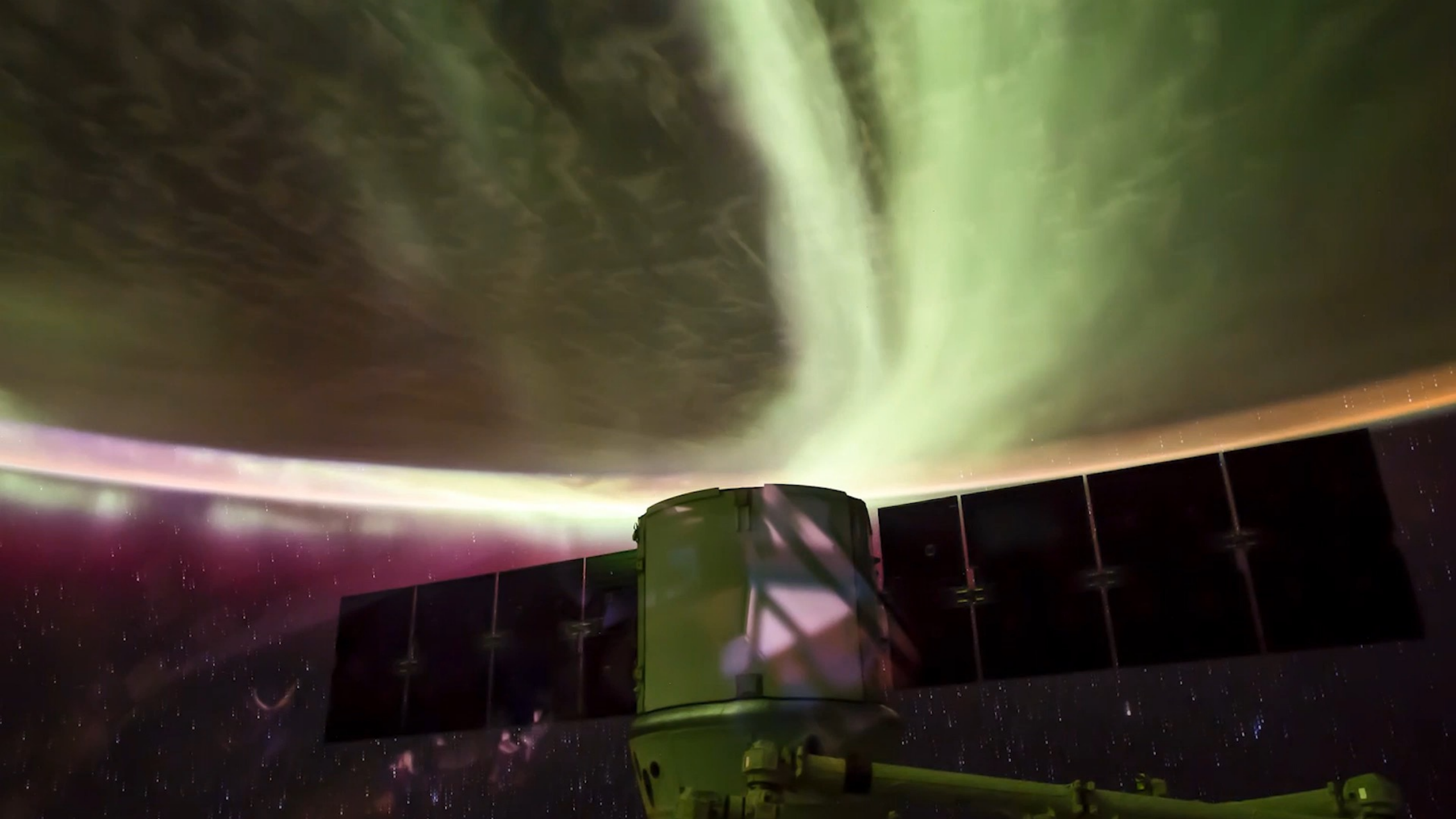
- The attack surface
- Importance of placement of verification/detection
- Defense in depth techniques
- Component isolation
- Software vulnerability management
- Zero Trust concepts

Science and Technology

From the DHS publication: A Cybersecurity Perspective to Addressing PNT Vulnerabilities, September 2022

Momentum Towards PNT Resilience

- US DOT Report in 2021 assessing 11 different technologies
- US Executive Order 13905 – Calls for federal procurement to include resilient PNT systems as part of the grants made available through the recent infrastructure bill. .
  - The order is expected to direct key federal agencies to begin including PNT resilience requirements in their procurements.
- Infrastructure Investment and Jobs Act funds enables state and local governments to implement PNT resiliency.
- European Union JRC report released in March 2023; highlighted NextNav exceeded all key benchmarks for resilient PNT; key recommendations include developing a system of systems, and for member states to dedicate spectrum for terrestrial PNT systems.



Thank You!

Twitter: @NextNav
Linkedin: @NextNav

NEXTNAV

Appendix

DOT Test Performance Summary

Positioning

Positioning	Accuracy
Static Outdoor Positioning*(1) (ground level)	~5.5 m
Airborne Positioning*(2)	3.3 m

*[1] 95th percentile 2D & 3D position accuracy (m) across all tests [2] 3D mean accuracy (m)

Timing

Timing	Accuracy
Static Outdoor Timing	7.1 ns
72 hr Static Bench Timing	23.1 ns

*[1] 95th percentile timing accuracy across all tests (ns)

2021 DOT Report Ranking GPS Backup Technologies

			TIMING[1]		POSITIONING[2]		TIMING[3]		PNT[4]		TIMING[5]		PNT[6]	
			Performance		Performance		Ground broadcast		Ground broadcast		Broadcast		Broadcast	
			Rank	Score	Rank	Score	Rank	Score	Rank	Score	Rank	Score	Rank	Score
NEXTNAV	UHF terrestrial RF	(920-928 MHz)	**1**	91	**1**	91	**1**	82	**1**	82	**1**	82	**1**	82
ECHO RIDGE	LEO commercial S-band	(2483.5-2500 MHz)	-	-	5	38	-	-	-	-	-	-	-	-
HELLEN	eLORAN terrestrial RF	(90-110k Hz)	6	62	-	-	3	66	-	-	4	66	-	-
opnt.	Fiber optic time service	(white rabbit PTP)	2	87	-	-	-	-	-	-	-	-	-	-
PHASORLAB	802.11 terrestrial RF	(2.4 HGz)	6	62	3	-	4	-	2	-	5	-	3	-
Satelles	LEO commercial L-band	(1616-1626.5 MHz)	4	78	2	78	-	-	-	-	2	80	1	82
serco	R-made terrestrial RF	(283.5-325 KHz)	-	-	-	-	-	-	-	-	-	-	-	-
SEVEN Solutions	Fiber optic time transfer	(white rabbit PTP)	3	84	-	-	-	-	-	-	-	-	-	-
SKYHOOK®	802.11 terrestrial RF	(900 MHz, 2.4 & 5 GHz)	-	-	4	-	-	-	-	-	-	-	-	-
TRX	UWB & IMU map matching	(3.1-5 GHz)	-	-	5	38	-	-	-	-	-	-	-	-
UrsaNav	eLORAN terrestrial RF	(90-110KHz)	5	69	-	-	2	70	-	-	3	70	-	-
GPS (SPS PS)	MEO government, L-band	(1575, 1227, 1176 MHz)	-	67	-	-	-	-	-	-	-	-	-	-

Ranking & score based on accuracy, availability, product readiness, resilience and security

Source: DOT Report: https://www.transportation.gov/sites/dot.gov/files/2021-01/FY%2718%20NDAA%20Section%201606%20DOT%20Report%20to%20Congress_Combinedv2_January%202021.pdf.

(1) Weighted score based upon accuracy, availability, product readiness, resilience and security.
(2) Weighted score based upon accuracy, availability, product readiness, resilience and security.
(3) Market readiness of Timing Performance using terrestrial RF broadcast.
(4) Mass market readiness for Position AND Timing using terrestrial RF broadcast.
(5) Mass market readiness of timing using RF broadcast.
(6) Mass market readiness for Timing AND Positioning using RF broadcast.