1. **Describe any public or private sector need for and/or dependency on the use of positioning, navigation, and timing, or any combination of these, services.**

   Collins Aerospace, a unit of Raytheon Technologies Corporation, is a leader in technologically advanced and intelligent solutions for the global aerospace and defense industry. Various aviation, military and critical infrastructure industries like nuclear power, railroads and government depend on our products to provide both navigation and communication capabilities that rely on PNT services. The Department of Homeland Security (DHS) has also recognized PNT as a cross dependency among 13 of the 16 critical sectors of the nation's infrastructure which range across financial, energy and telecommunications networks. In addition, DHS has designated PNT (Positioning, Navigation, and Timing) services a "National Critical Function."

2. **Identify and describe any impacts to public or private sector operations if PNT services are disrupted or manipulated.**

   The impacts to Collins Aerospace's products and services that support both public and private sector operations can be roughly categorized as navigation or time-based. A few examples are provided below.

   Navigation: As our products provide aviation navigation services that support all phases of flight operations, disruption/manipulation of PNT could result in incorrect or non-existent position information for aircraft. These impacts can be seen across the board where a loss of GPS based navigation can impact the availability of RNP (Required Navigation Performance) at the aircraft level and could also result in a loss of ADS-B capability on the airplane. At this point, depending on aircraft equipage and area of operation, we could see impacts to both navigation and surveillance domains in CONUS airspace.

   Time: Many communication technologies rely on a time-division multiplexing approach that require synchronization between transmitters and receivers. Often provided by a beacon based on GPS-derived time, disruption/manipulation of PNT could result in an inability to communicate necessary/critical information.

   Additionally, many network services use time to create server logs, coordinate activities and implement cybersecurity measures. Erroneous time could result in an inability to authenticate, communicate and coordinate due to expired security certificates and an incorrect interpretation of network events.

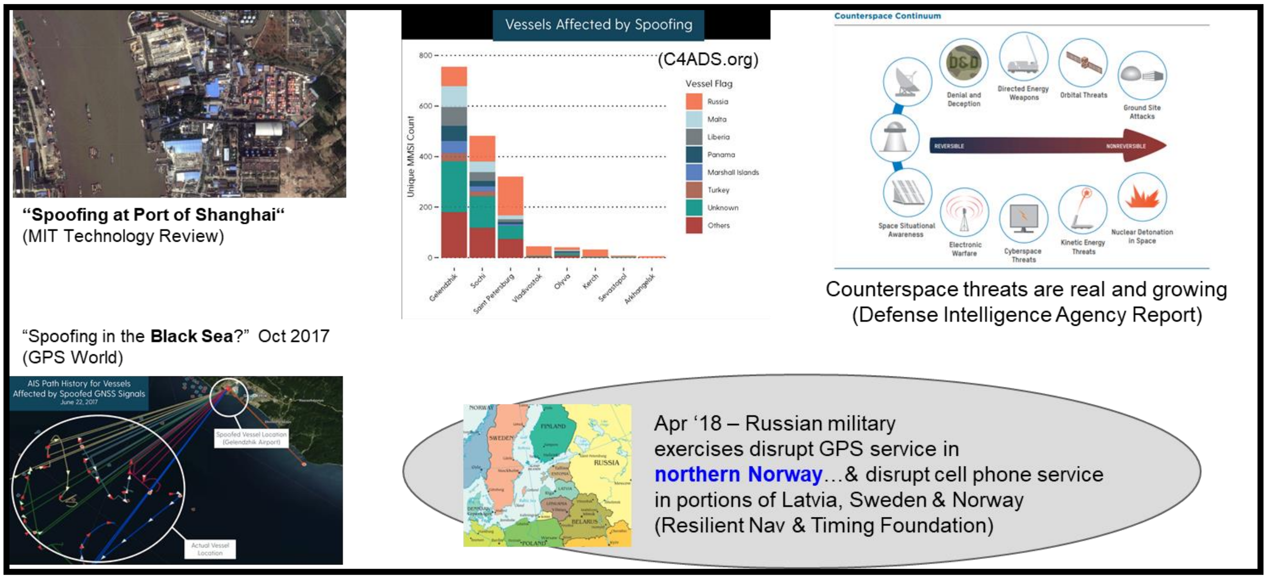
3. **Identify any standards, guidance, industry practices and sector specific requirements referenced in association with managing public or private sector cybersecurity risk to PNT services.**

Collins Aerospace uses aviation industry standards like RTCA DO-326A, DO-355 and DO-356A as well as internal/proprietary standards and requirements to manage cybersecurity risks to our systems and services.

Additionally, many of our ground-based networks use COTS components (e.g. certificates, VPNs, time distribution) that utilize common information technologies practices related to cybersecurity and intrusion detection/prevention. In conjunction with an established Risk Management Framework (RMF), a multi sensor layered approach to address PNT threats is seen as the most viable method to address the gamut of threats as applied to relevant SWaP constrained applications.

4. **Identify and describe any processes or procedures employed by the public or private sector to manage cybersecurity risks to PNT services.**

The contested electromagnetic environment and its effect on positioning, navigation and timing (PNT) technologies has evolved greatly in recent years with widespread disruption being reported across the globe. While the historical challenges of unintentional and co-site interference persist, adversaries have now developed sophisticated denial and deception threats including jamming, spoofing, and cyber technologies which have been shown to significantly impact legacy PNT systems. Due to the widespread adoption and dependence of Global Navigation Satellite Systems (GNSS) and other PNT services by critical infrastructure, these new threats pose a risk to the national and economic security of the United States.



**"Spoofing at Port of Shanghai"**
(MIT Technology Review)

Counterspace threats are real and growing
(Defense Intelligence Agency Report)

"Spoofing in the **Black Sea**?" Oct 2017
(GPS World)

Apr '18 – Russian military exercises disrupt GPS service in **northern Norway**…& disrupt cell phone service in portions of Latvia, Sweden & Norway
(Resilient Nav & Timing Foundation)

***Publications Showing Recent GNSS Disruption across the Globe***

*Figure 1: Global GNSS disruptions*

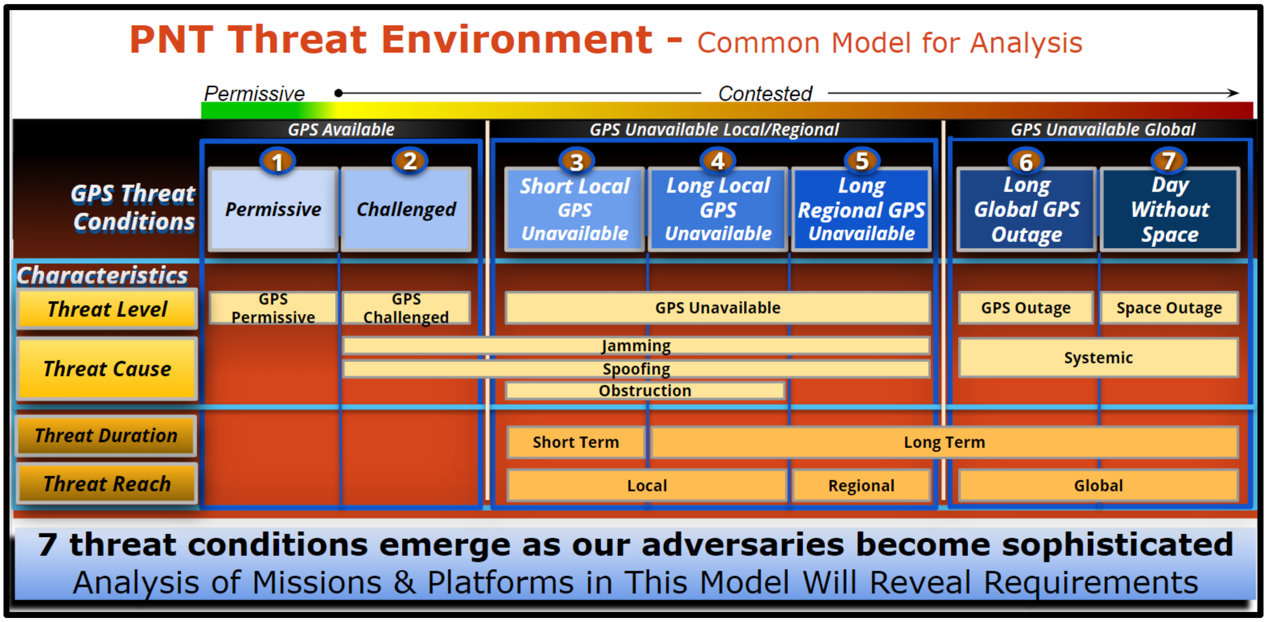
To aid in an industry discussion of PNT threats, their effects, and potential mitigation solutions Collins Aerospace has found it beneficial to begin with the definition of a common threat model derived from real world intelligence. Such a model helps to refine and focus the discussion and facilitate a common understanding of the problem to be solved among government and industry participants. We encourage the government to adopt a threat model to aid in the problem space definition as it relates to critical infrastructure. As a starting point for this model and discussion we present below an example threat model that was developed for the US Army Assured PNT programs.

*At a high level the US DoD identified two capability gaps that have resulted from the evolving electronic battlespace [U.S. Army* Training and Doctrine Command *(TRADOC) ICD]. These capability gaps are:*

1. Access gap – PNT information is not available in impeded conditions
2. Integrity gap – inability to determine validity and accuracy of PNT information

Closing these gaps is the primary motivation for the Army's vision of Assured PNT, and directly applicable to the mitigation of risks to critical infrastructure within the US.

Since GNSS continues to be a foundational component of PNT systems due to its global, all weather, high performance and low SWaP characteristics, the GNSS service is a primary target of electronic threats and the basis for this example threat model. However the model would apply generally to any RF based PNT service and a similar model could be created to address broader PNT technologies and systems.



**PNT Threat Environment - Common Model for Analysis**

| | GPS Available | | GPS Unavailable Local/Regional | | | GPS Unavailable Global | |
|---|---|---|---|---|---|---|---|
| **GPS Threat Conditions** | 1 Permissive | 2 Challenged | 3 Short Local GPS Unavailable | 4 Long Local GPS Unavailable | 5 Long Regional GPS Unavailable | 6 Long Global GPS Outage | 7 Day Without Space |
| **Characteristics** | | | | | | | |
| **Threat Level** | GPS Permissive | GPS Challenged | GPS Unavailable | | | GPS Outage | Space Outage |
| **Threat Cause** | | Jamming<br>Spoofing | Obstruction | | | Systemic | |
| **Threat Duration** | | | Short Term | Long Term | | | |
| **Threat Reach** | | | Local | | Regional | Global | |

**7 threat conditions emerge as our adversaries become sophisticated**
Analysis of Missions & Platforms in This Model Will Reveal Requirements

***Common PNT Threat Model for Analysis***

*Figure 2: Common PNT Threat Model*

Once a refined understanding of the threat environment is achieved (based on the construct depicted in Figure 2), this model can be further used to depict technologies / solutions and how they apply across the threat conditions.

In the context of the threat model depicted above, our systems use redundant and dissimilar technologies to manage the cybersecurity risks to PNT services. For example, our communication systems may use multiple techniques to derive and maintain their network timing besides GPS-based methods. This mitigates the inability to authenticate, communicate and coordinate due to nonfunctioning cybersecurity measures like certificates and cryptography keys dependent on accurate time. However, if this threat persists; the loss of timing to support these operations could have undesirable impacts. Collins is glad to discuss this trade space further with NIST as we move forward.

5. **Identify and describe any approaches or technologies employed by the public or private sector to detect disruption or manipulation of PNT services.**

Collins Aerospace has the capability to deliver integrated systems that provide robust position and timing for both ground based and airborne systems. For example, our airborne products utilize redundant and dissimilar technologies (e.g. inertial measurement units) that augment position information through various levels of GPS Inertial integration. Similar sensor fusion capabilities are available for a variety of ground based applications.

One of the technologies of interest is the ability to detect threats to GPS in the electromagnetic environment. Collins navigation systems include a CRPA with antenna electronics to provide GPS anti-jam capability. This same equipment also monitors the RF environment and indicates when GPS jamming is detected, providing situational awareness to the platform and users. The Collins jamming detection capability uses direct sensing of the RF environment to detect jamming, providing a sensitive and accurate means to detect jamming and determine the power level of jamming that is impacting the navigations system.

In addition to detecting GPS jamming threats, the Collins anti-jam system also determines the direction to jamming and high-power spoofing threats using a direction-finding algorithm based on the classic multiple signal classification methodology. This algorithm uses signal processing data generated by the anti-jam antenna electronics using data from multiple phase centers in the antenna array to determine RF threat information including direction to threat (azimuth/elevation), threat transmit frequency and threat RF bandwidth.

Multiple observations of the direction to RF threats (Figure 3) can be combined to determine location of threats. For example, an individual platform could fly a path to collect a set of direction measurements to determine threat locations, or observations from multiple platforms could be combined to determine threat locations, as shown in the figure below. This threat direction finding capability allows RF transmitters that interfere with GPS navigation to be located and mitigated.

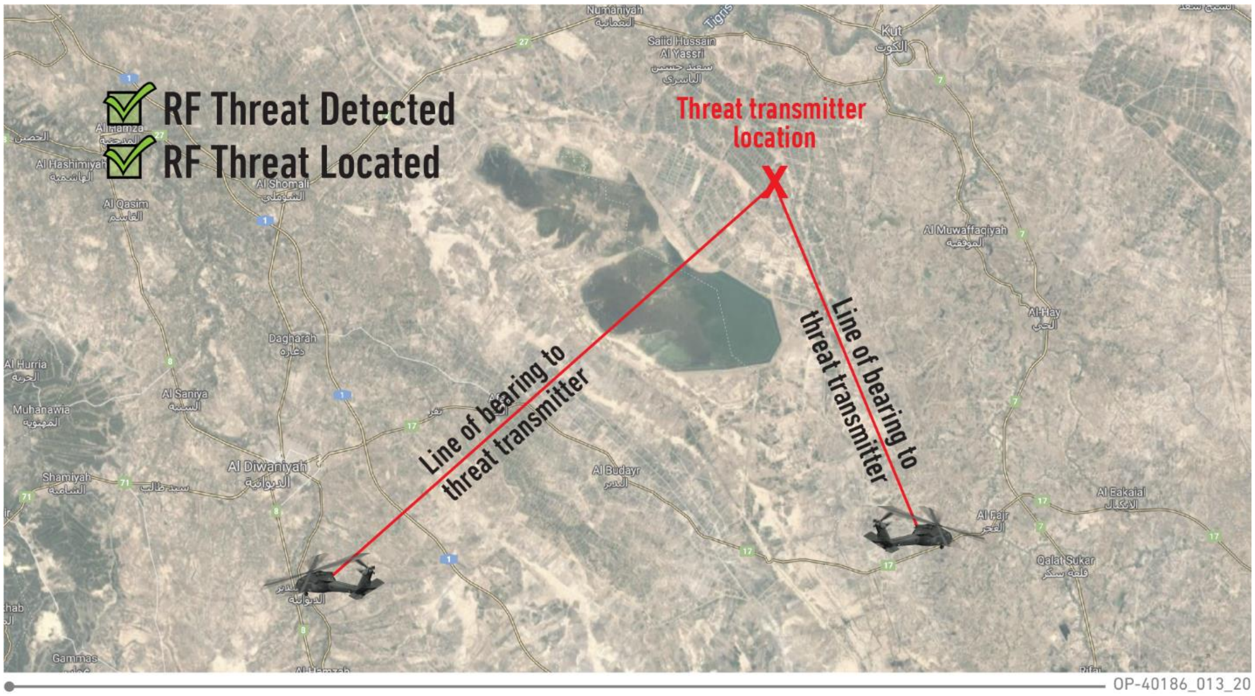


*Figure 3: Threat Detection*

*Collins brings advanced situational awareness capabilities for detection and location of RF threats.*

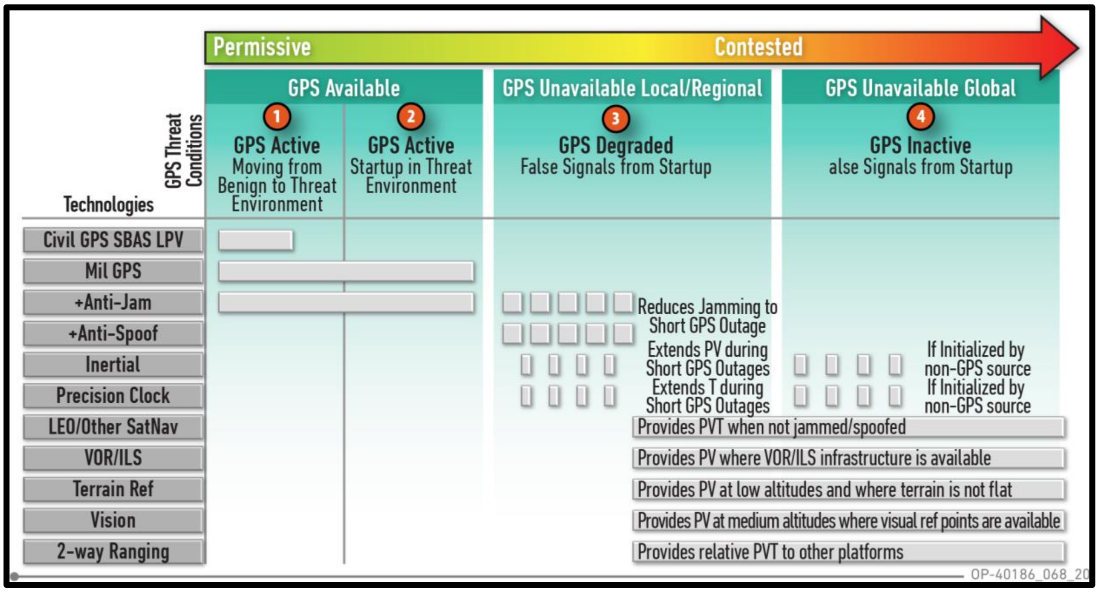
Collins Aerospace is also developing advanced detection and direction finding capability for low power GPS spoofing signals. Like GPS signals, these spoofing signals are at a power level that is below the thermal noise floor and so they are undetectable by traditional RF power detectors. However they pose an even more substantial threat to GPS receivers than the high power threat signals. Through the use of advanced GPS and GNSS correlation algorithms and multi-sensor fusion algorithms these signals can be detected and a line of bearing to the transmitting source can be determined.

Other single antenna GNSS based spoofer detection techniques have been developed and can be considered for use in applications that are unable to support CRPA's (either due to policy and/or SwaP limitations).

6. **Identify any processes or procedures employed in the public or private sector to manage the risk that disruption or manipulation to PNT services pose.**

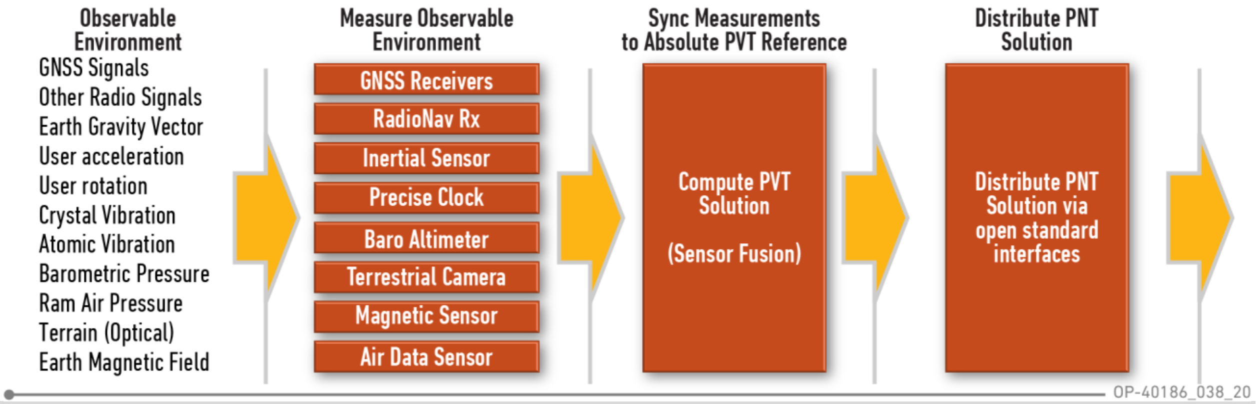
Collins is actively collaborating with the Army PNT program office and the Army Futures Command PNT CFT to develop the next generation of multi-sensor assured PNT systems to support multi-domain operations and mitigate the evolving electronic threats that warfighters are facing today. These mitigation technologies are directly applicable to the US critical infrastructure risk.

While there is no single technology that can replace GNSS and provide Assured PNT for the general use case and under all threat conditions, there are several alternate positioning and timing technologies each with specific benefits and limitations. Therefore in many cases a layered approach to PNT threat mitigation is needed in which multiple technologies are combined in a way to complement each other for the best overall assured PNT solution. These technologies are typically optimized for the specific platform. For example an aircraft, ground vehicle, and water vehicle typically need to use different sensing technologies to achieve assured PNT capability.


Permissive
Contested
GPS Available
GPS Unavailable Local/Regional
GPS Unavailable Global
GPS Threat Conditions
Technologies
1
GPS Active
Moving from Benign to Threat Environment
2
GPS Active
Startup in Threat Environment
3
GPS Degraded
False Signals from Startup
4
GPS Inactive
alse Signals from Startup
Civil GPS SBAS LPV
Mil GPS
+Anti-Jam
+Anti-Spoof
Inertial
Precision Clock
LEO/Other SatNav
VOR/ILS
Terrain Ref
Vision
2-way Ranging
Reduces Jamming to Short GPS Outage
Extends PV during Short GPS Outages
Extends T during Short GPS Outages
If Initialized by non-GPS source
If Initialized by non-GPS source
Provides PVT when not jammed/spoofed
Provides PV where VOR/ILS infrastructure is available
Provides PV at low altitudes and where terrain is not flat
Provides PV at medium altitudes where visual ref points are available
Provides relative PVT to other platforms
OP-40186_068_20

***Example Multi-sensor PNT Access for a Specific Platform***

To enable this layered approach and accomplish threat mitigation a flexible multi-sensor architecture is needed which is able to make use of a variety of sensors chosen to optimize performance for each platform or use case. Collins Aerospace navigation sensor fusion technology is based on this principle, and provides reliable access to high integrity PNT in threatened environments.  It is important to note that the threats to PNT continue to evolve over time



***Navigation Sensor Fusion Architecture***

*Complimentary navigation technologies are fused together to provide one source of continuous trusted PNT in GNSS degraded and GNSS denied environments.*

*Figure 4: Navigation Sensor fusion architecture*

The Collins Aerospace navigation sensor fusion architecture (Figure 4) embraces open standards such as PNT Architecture Standard (PNTAS), All Source Positioning and Navigation (ASPN), Future Airborne Computing Environment (FACE), the Vehicle Integration for C4ISR/EW Interoperability (VICTORY) and the Army PNT Reference Architecture to encourage collaboration and technology sharing across industry. This open system architecture approach results in a modular, scalable and upgradeable suite of capabilities that are easily upgraded to address a continuously evolving threat.

Redundant and dissimilar technologies are used to detect disruption/manipulation and ensure fault tolerance. For example, position and time derived using GPS methods on an aircraft are verified using other methods such as inertial measurement units and local, real-time clocks.

Proprietary algorithms note the discrepancies in information and determine true position and time even when faced with unreliable PNT services. This ensures continuous operation for critical systems that support aviation, military, nuclear power, railroads and government services.

7. **Identify and describe any approaches, practices, and/or technologies used by the public or private sector to recover or respond to PNT disruptions.**

Collins Aerospace has numerous proprietary systems and methods (e.g. multi-antenna, multi-frequency, multi-constellation receivers) that are capable of providing robust and validated satellite navigation and timing for high-value critical applications.

GNSS continues to be a foundational component of navigation systems due to its global, all weather, high performance and low SWaP characteristics. As such we categorize threat mitigation technologies into three primary categories: GNSS Receivers, GNSS Protection and Non-GNSS Augmentation. Collins solution uses all of these navigation technologies in a layered approach to close the PNT access gap
.

For example, in a military application the first layer of defense is the use of a modernized (M-code) GPS receiver, which includes jamming resistance, blue force electronic attack compatibility and spot beam compatibility. While commercial applications may not have access to the M-code signal, some of these technologies may be of interest when investigating the solution space for the US critical infrastructure. In addition there is benefit that can be gained through the simultaneous use of multiple GNSS constellations to provide signal diversity to the navigation system. The modern GNSS receiver by itself can achieve PNT access in benign and minimally contested electromagnetic environments and provides a strong foundation for the more advanced navigation capability required by some platforms.

The next layer of defense, GNSS protection, is accomplished using anti-jam antenna array technology. Through the use of advanced nulling and beamforming algorithms anti-jam antennas reduce the area of GNSS denial due to jamming by orders of magnitude and allow the navigation system to continue to utilize all sensors throughout the mission. Collins navigation systems with industry leading anti-jam antenna technology are currently being flown in theater to support urgent operational needs and provide mission effectivity in highly contested electromagnetic environments.

The final layer of defense, Non-GNSS Augmentation, is performed by our navigation sensor fusion technology. No single sensor can provide full navigation capabilities in all circumstances, so multiple technologies are chosen which complement each other to create a comprehensive navigation system that is fully capable. For example, GNSS denied navigation using terrain referenced navigation is optimally performed at low altitudes while vision-based navigation using map matching is optimally performed at mid-range altitudes. Together they cover a substantial vertical operational space, but not when flying over featureless terrain such as ocean or desert. Other sensors must be relied upon to fill in the limitations of individual technologies. Our sensor fusion capability uses all available sensors to continue navigating when GNSS is degraded or denied.

Given the nature of the technologies discussed above, some of the implementations are are proprietary/export-controlled and Collins Aerospace will be glad to discuss tailoring these capabilities to relevant use cases of interest with NIST as we move forward.

8. **Any other comments or suggestions related to the responsible use of PNT services.**

As indicated above, Collins Aerospace has developed numerous proprietary approaches and technologies to mitigate the effects of both purposeful manipulation (e.g. spoofing) and environmental disruption (e.g. solar activity, spectrum interference) of PNT services. Collins Aerospace looks forward to further discussions with NIST on how these techniques can be tailored and applied to address a variety of use cases of interest to NIST and its partners.