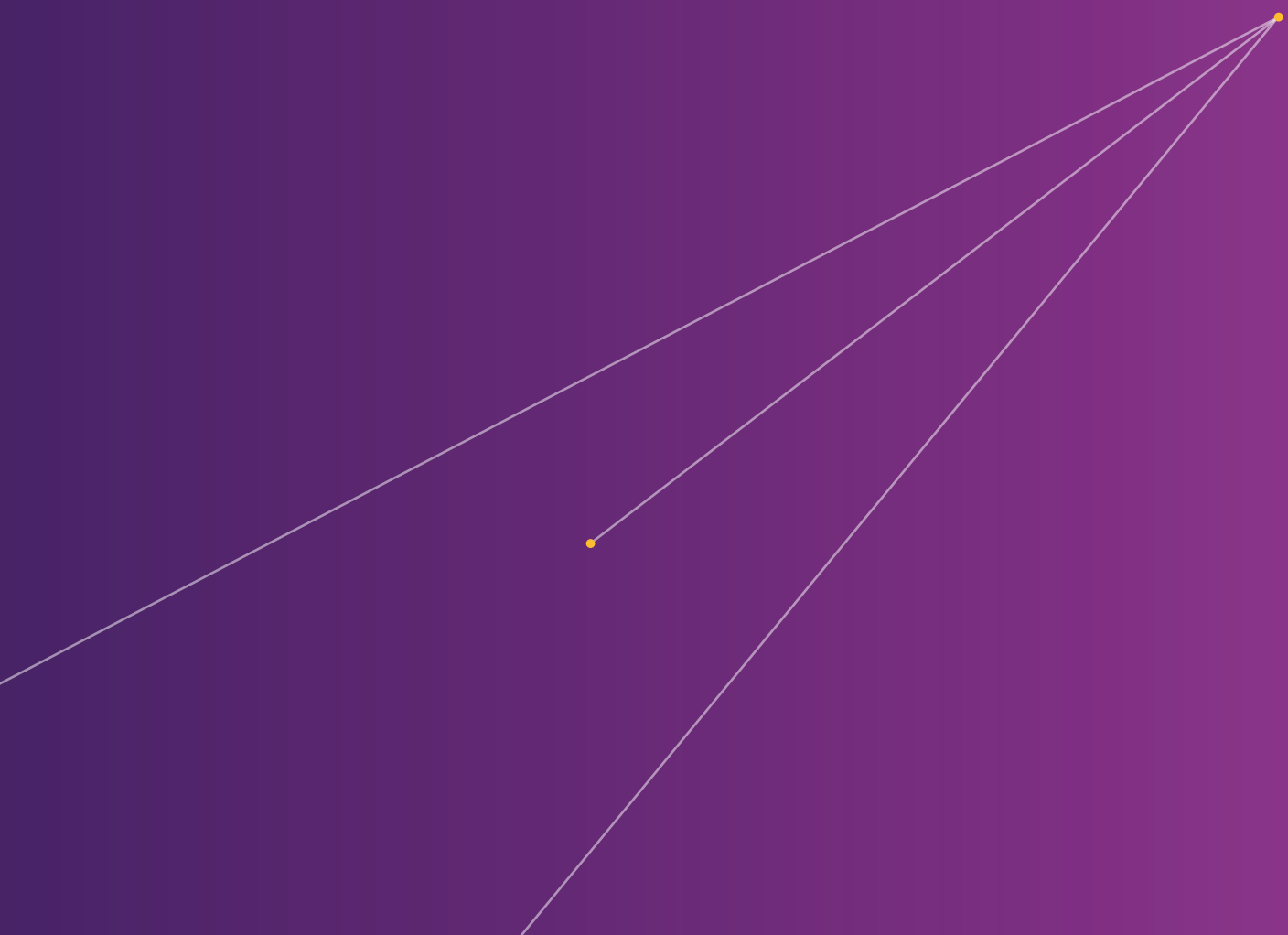
Booz | Allen | Hamilton®

VIEWPOINT

# MORE RESILIENT POSITIONING, NAVIGATION AND TIMING (PNT) THROUGH OPEN ARCHITECTURE AND ANALYTICS

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER



# MORE RESILIENT POSITIONING, NAVIGATION AND TIMING (PNT) THROUGH OPEN ARCHITECTURE AND ANALYTICS

## THE CHALLENGE: Resilient PNT is Hampered by Technical and Prioritization Hurdles

Today, more than 700 types of platforms, networks, and communications systems across the military and intelligence enterprise rely upon Global Positioning System (GPS) signals for PNT information. GPS-delivered PNT information is the connective tissue that enables today's digitized warfighters to navigate, communicate, synchronize, and operate with unprecedented situational awareness, speed, and precision across all battlefield domains. As one military planner put it, "GPS is fundamental to everything we do. It is a part of our plumbing today."[1]

Yet GPS — and the PNT information it provides — are increasingly vulnerable to a growing array of jamming and spoofing tactics that current or potential adversaries can employ with relative ease and at minimal cost. When GPS-delivered PNT information is disrupted, many of today's modern military and intelligence operations can be effectively blinded and desynchronized. And many systems, such as some communications systems that critically depend on GPS' precise timing information, may not be able to operate at all.

The Department of Defense has invested heavily in GPS to improve the resilience of the system itself to the maximum extent possible. In the last 20 years alone, GPS has added new military and civilian signals, new cryptography, new navigation data messages, better accuracy, more signal power, better satellites, an improved control segment, and significantly improved user equipment and associated anti-jam antennas. However, there are limits to the resilience of any satellite navigation system — even the best — that result in vulnerabilities that cannot be mitigated by GPS alone.

To address this, defense and intelligence organizations are investing heavily to develop more resilient PNT capabilities — in the form of upgrades, augmentations, and alternatives to GPS — to ensure systems and platforms remain mission-ready, even in contested environments. In many cases, adding an additional PNT sensor to an existing GPS-based navigation system is the solution. Many of these improvements rely on mature technologies, but while defense and intelligence organizations are making strides, it is clear that current approaches to acquire and field resilient PNT cannot keep pace with the scale and severity of current and emerging threats. Two sets of issues hamper progress; one set is technical in nature, while the other set concerns the prioritization of how, when and where to modernize.

## TECHNICAL ISSUES

The primary technical issue is that because weapon, communication and other systems are typically closed and proprietary, it is difficult for defense and intelligence organizations to deploy improved PNT approaches or technologies at scale.

The systems and their PNT capabilities tend to be closely integrated, and often only the original equipment manufacturer (OEM) or a certified third-party is capable of performing upgrades, modernization, or maintenance on the PNT components within those systems.

This predicament vastly complicates and overburdens the task of introducing new approaches and technologies that can deliver resilient PNT capabilities — not only today but also in the future, as promising new PNT technologies emerge.

The closed, proprietary nature of many defense and intelligence systems also poses acute affordability issues. Upgrading PNT capabilities for these systems is typically a highly customized endeavor, and, consequently, very costly to do even one at a time, let alone at scale. Also, closed and proprietary PNT components are often incompatible with other systems, and so it is difficult to pursue an economical strategy of sharing and interlinking PNT capabilities across multiple systems and platforms.

In addition, program offices deploying PNT-enabled systems often struggle to accurately define their PNT requirements, as they may not have performed the necessary analysis to determine their threshold requirements and simply defaulted to the GPS requirements as their baseline, sometimes referred to as the technical baseline. That information is critical to understanding the trade-offs that come with various upgrade options, and the best way to join the right PNT capability with the right system at the right cost.

## PRIORITIZATION ISSUES

The second set of issues associated with improving PNT resilience is around prioritizing where, when, and how to direct limited resources. In many cases, organizations lack evidence-based strategies and frameworks to guide these decisions. The process of prioritizing PNT modernizations and upgrades is highly complex. Factors include the operational importance of a platform or system, the severity of a platform's PNT vulnerabilities, the affordability of the solution, and the degree of convenience associated with implementing a solution.

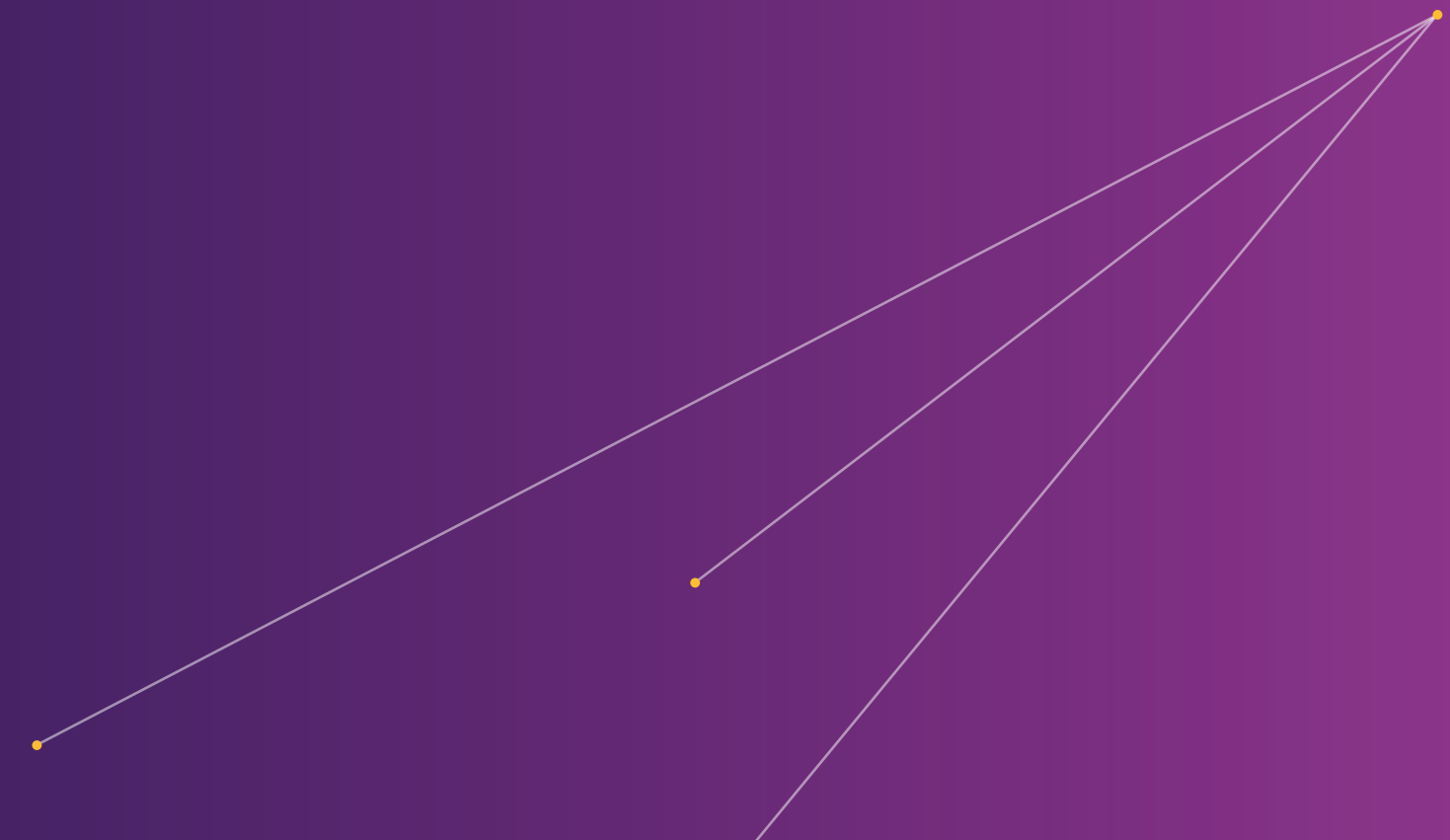
There is additional complexity when assessing PNT needs and vulnerabilities across an entire ecosystem of networks, platforms, and systems that support battlefield operations. An example is the "kill chain" used to destroy enemy targets, in which separate but interlinking systems are responsible for the find, fix, track, target, engage, and assess functions of an attack. In many cases, critical PNT vulnerabilities are introduced during system integration and cannot easily be found, especially as a kill chain often consists of multiple systems operated by different organizations and sustained by different OEMs.

Determining which systems require attention – and when – is only one piece of the puzzle. There is also the issue of understanding exactly how to improve the resilience of PNT capabilities of various systems. Each defense and intelligence system and platform has specific PNT needs and tolerances. For example, how precise and robust must the needed PNT capability be for a given system? Is an extensive modernization necessary with a system that is scheduled to be replaced in two or three years? These kinds of critical questions carry significant readiness as well as affordability implications.

The issue is made more difficult because program offices often operate in stovepipes – they may have a good understanding of the PNT needs and vulnerabilities in their own systems, but not of how those needs and vulnerabilities play out across integrated systems. So, while program offices may comply with leadership directives for PNT resiliency — such as by installing M-code receivers in their systems — they may not end up with the kinds of resilient PNT capabilities they will truly need in degraded battlefield environments unless the system-of-systems in which they operate is assessed as a whole.

The net effect of these technical and prioritization issues is that PNT modernization efforts are progressing, but only incrementally. The scale and urgency of the challenge demands a far more aggressive strategy.

DEFENSE AND INTELLIGENCE ORGANIZATIONS ARE INVESTING HEAVILY TO DEVELOP MORE RESILIENT PNT CAPABILITIES — IN THE FORM OF UPGRADES, AUGMENTATIONS, AND ALTERNATIVES TO GPS — TO ENSURE SYSTEMS AND PLATFORMS REMAIN MISSION-READY, EVEN IN CONTESTED ENVIRONMENTS.



# OUR PERSPECTIVE: Open Architectures and Data-Informed Prioritization Deliver Resilient PNT Faster and More Affordably

Two fundamental steps are needed to overcome the challenge to resilient PNT:

- Transition PNT capabilities to open architecture environments; and
- Take advantage of data and analytics to prioritize where, when, and how to modernize PNT.

## WHY OPEN ARCHITECTURES ARE CRITICAL

Transitioning PNT capabilities to open architecture environments leads to significantly greater resiliency at lower cost. With open architectures, technologies can be rapidly upgraded or replaced by swapping out one component for another component. It is difficult to achieve this "plug-and-play" capability when systems and platforms are closed and the PNT components within them are proprietary and closely integrated to their respective systems. Open architectures eliminate this need for tight coupling and enhances PNT resiliency in several important ways, as follows:

First, open architectures enable systems and platforms to have ready and rapid access to new PNT technologies as they emerge. This means PNT solutions would no longer be limited to the confines of a system's particular proprietary environment — instead, program offices can incorporate solutions, wherever they originate, that are most optimal for addressing the warfighter's mission objectives. For example, moving beyond simply providing access to alternative signals or automated celestial navigation systems, PNT capabilities can be more quickly and easily upgraded with new functional attributes, such as a greater ability to detect whether PNT information is being degraded or spoofed, to resist or recover from such attacks, or to acquire supplemental PNT sources when needed. Being able to plug a new PNT sensor onto a 'plug and play' platform would be considerably faster than having to redesign each individual platform or system to accommodate such an upgrade.

Second, costs are lowered because laborious, customized PNT upgrades or replacements on individual systems — which often necessitate the system's redesign to accommodate the new component — are no longer necessary. As a result, cost savings can be reinvested in alternative PNT capability, as needed. Again, this is because when PNT components are not housed in closed, proprietary environments, it is less costly and time-consuming to make modifications, which could include the addition of backup or supplementary PNT sources.

## WHY ANALYTIC-INFORMED PRIORITIZATION IS CRITICAL

Every system and platform cannot be modernized with improved PNT capability at once. Due to budget and time constraints, some systems can be modernized, some can get only incremental updates, while still others must necessarily go without PNT upgrades. This means that, at any given time, the 700-plus types of PNT-enabled systems and platforms that service the battle space will operate at various levels of readiness in a degraded PNT environment.

With this in mind, planners need to fully understand the battlefield consequences of their options when making complex prioritization decisions. For example, how will a decision to modernize — or, alternatively, to incrementally augment — the PNT

capabilities of a squadron of UAVs play out in terms of risk and overall battlefield performance?

This is where data science and advanced analytics can play a critical role in delivering important insights. Data models can quickly and reliably weigh the many factors that play a role in prioritizing available options. For example, organizations can employ simulations to identify the most critical PNT vulnerabilities that arise in various battlefield scenarios, thereby informing decisions about which systems to address — and in what sequence.

Such an analytic-informed approach incorporates frameworks, methodologies, and data-derived insights to identify and assess options, and manage the accompanying risks. Decisions are better aligned to readiness and budget needs, and based on clear, objective assessments of the data. They are also more defensible in budget deliberations, and less prone to potential readiness blind spots that might arise from a less rigorous, methodical approach.

These two steps — transitioning PNT capabilities to open architectures and prioritizing modernization through data and analytics — are critical to achieving scalable and affordable resilient PNT.

However, these steps are not easily done. They require robust capabilities and competencies in data analytics, modeling and simulation, cybersecurity, engineering and design; much experience with open architectures and system integration; extensive staff reach throughout the military and intelligence enterprise; vast mission and system expertise; and, importantly, the lack of potential organizational conflicts of interest.

## OVERCOMING THE CHALLENGE TO RESILIENT PNT

- Transition PNT capabilities to open architecture environments.
- Take advantage of data and analytics to prioritize where, when, and how to modernize PNT.

# OUR APPROACH: Delivering Resilient PNT in Four Steps

The path toward PNT resilience will vary with each organization — its mission portfolio, the state of its existing PNT environment, its resiliency goals and constraints, and other factors all contribute to the pace and contours of each effort. Booz Allen helps defense and intelligence organizations implement open architecture approaches and prioritize modernization efforts to address their unique PNT requirements.

Booz Allen brings an analytic approach through a proven methodology that focuses on assessment, prioritization strategy, proof of concept, and implementation.

## ASSESSMENT

We start with an environmental diagnostic and baselining exercise to assess all aspects of an organization's mission portfolio, PNT environment, modernization goals, and constraints. This includes conducting end-to-end assessments of all PNT-enabled systems and platforms that support mission-essential tasks to understand critical interdependencies and potential vulnerabilities.

Assessment teams work with program management offices and system OEMs to develop an in-depth technical understanding of affected system architectures and existing PNT capabilities. This technical knowledge — or "baseline" — informs the design of an open architecture transition plan. Assessment teams also assess and weigh all factors to be considered in deciding which systems are to be addressed, how they are to be addressed, when, and in what sequence.

## PRIORITIZATION STRATEGY

Next, we develop an integrated, milestone-based strategy that outlines a risk-managed, prioritized plan for addressing PNT resilience across the client-defined portfolio of affected systems and platforms. Critical in this stage is the development, testing, and validation of prioritization models. Booz Allen works with organizations to develop these models by employing client input, vulnerability assessments, data analytics, operational modeling and simulations, budget assessments, and other activities. This work will inform decisions about how individual PNT-enabled systems and platforms will be addressed, whether through augmentation, supplemental data, upgrades, a more comprehensive modernization, or another approach.

The prioritization strategy includes a roadmap for transitioning the PNT capabilities of affected systems and platforms to open architecture environments. Project teams for each affected system and platform develop conceptual open architectures to enable the decoupling and enhancement of existing PNT capabilities within priority systems.

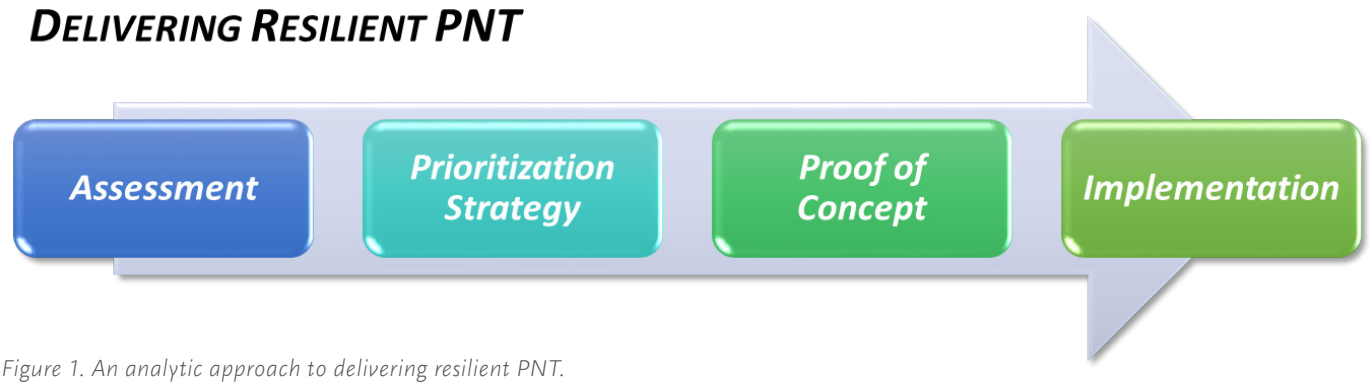



*Figure 1. An analytic approach to delivering resilient PNT.*

## PROOF OF CONCEPT

To help validate critical components of the integrated strategy, Booz Allen employs test beds and design labs to conduct proof of concept exercises. The key components of this phase consist of validating the technical feasibility and functional effectiveness of: conceptual open architectures; planned PNT enhancements; and the decoupling and recoupling of PNT components. From these proof of concept exercises, evaluation teams develop recommendations for revisions to the integrated strategy and for the next step, implementation.

## IMPLEMENTATION

The final step focuses on assisting project teams install and validate PNT open architectures based on recommendations informed by prioritization assessments and proof of concept evaluations. Once open architectures are in place and validated, project teams proceed to scale PNT enhancements and capabilities — through the decoupling and recoupling process — that were validated in the proof-of-concept phase across the defined portfolio of systems and platforms. Project teams also ensure that new and enhanced PNT capabilities are well integrated with organizational policies, operational protocols, training, doctrine, compliance, oversight, logistics, and culture.

## BOOZ ALLEN: Your Essential Partner In Resilient PNT

Delivering resilient PNT capability to where it is most urgently needed, in the most efficient and affordable way, requires a wide array of capabilities and competencies. Booz Allen possesses unrivaled experience and expertise in every aspect of PNT. As industry leaders in open architectures and other digital solutions, and in next-generation cybersecurity and advanced analytics, we are pioneering new approaches to PNT resilience. We bring this broad range of technical expertise together with our consulting mindset, as well as with the domain and mission knowledge we've gained through more than 75 years of helping defense and intelligence agencies solve their most complex problems.

Booz Allen has long been a champion of open architecture to achieve system and platform interoperability and integration. Our more than 5,000 digital strategists, architects, developers, and user-experience professionals have worked closely with agencies in all corners of government to develop enterprise-wide digital solutions that are open, agile, and secure.

In addition, Booz Allen is at the forefront of advanced analytics, data science, artificial intelligence, and machine learning. Our data scientists – many of them among the earliest members of the profession – continue to invent breakthrough technologies and analytic approaches, transforming how business and government operate. We now have nearly 900 data scientists – one of the world's largest such teams – whose expertise reaches across every federal sector, including defense, intelligence, and homeland security. This extensive expertise enables Booz Allen to develop innovative data models that can effectively guide planners through the complex calculus of prioritizing their PNT modernization needs.

Booz Allen is also a recognized global leader in all dimensions of cyber, including the fast-growing subset of PNT vulnerabilities and threats. Our team of 5,000 cybersecurity experts, one of the world's largest, pioneered many of the most advanced approaches used in government and business today. We have unmatched expertise in the federal space, particularly in the defense and intelligence communities. For example, we are one of the few firms accredited by the National Security Agency to handle incident response. Our work across all government and commercial sectors gives us an unparalleled understanding of client missions, threat environments, and data and allows us to deliver PNT capabilities that are resilient in the face of active threats.

Our business model allows for rapid and seamless integration of these and other skillsets to deliver the most advanced PNT resilience solutions. And unlike the OEMs model, Booz Allen is free of potential organizational conflicts of interest. This enables us to deliver balanced, independent assessments of problems and solutions, and assist clients in developing and executing effective PNT modernization strategies that incorporate best-of-breed solutions that fit their missions, cultures, and budget constraints.

# OUR EXPERT

## For more information please contact our expert:

**Kevin Coggins**
*Vice President*
*Coggins_Kevin@bah.com*

## NOTES

*1. Capt. Mark Glover, program manager for the Navy's Communication and GPS Navigation Program Office, as quoted in "Beyond GPS: The Navy's plan for assured position, navigation, timing," Barry Rosenberg, C4ISR & Networks, Sept. 4, 2015.*

**About Booz Allen**

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.