Government Business Council

Managing Risk in a Tech-Centric Future

A Discussion on the Challenges to Adopting Mission-Critical Technologies

April 2023

INTRODUCTION

To avoid fraud, waste, and security risks, the federal government has created authorization processes for agencies looking to adopt new technologies. While preventing fraud, wasteful spending, and security breaches is undoubtedly necessary, mandatory authorization processes can create other, unintended risks. These processes can limit and decelerate the adoption of new mission-critical technologies needed by agencies. However, facilitating faster processes could create a greater balance between operation and security risks. To better understand how The Department of Defense (DoD) balances these risks while managing complex competing priorities, policies, and resource constraints, the Government Business Council (GBC) partnered with Motorola to interview the following experts.

THE EXPERTS

COL DAVID LAMY
Chief Information Officer, Army Futures Command Headquarters (AFC CIO)

DAVID DOCIMO
Army Futures Command Headquarters Directorate of Operations, Plans, and Experimentation and Assistant Chief of Staff (AFC G3/5/7)

JIM THOMSON
Deputy Director, Future Vertical Lift Cross-Functional Team (FVL CFT)

TIM SELPH
Deputy Director, Network Cross-Functional Team (N CFT)

MAJ BRIAN SZCZEPANEK
Deputy Chief of Operations, Next Generation Combat Vehicle Cross-Functional Team (NGCV CFT)

BRIDGETT SITER
Communication Director, Soldier Lethality Cross-Functional Team (SL CFT)

MARK CURRY
Computing Lead, Synthetic Training Environment Cross-Functional Team (STE CFT)

THE INTERVIEWS

The following responses have been lightly edited by GBC for brevity and clarity.

In your opinion, are federal authorization processes (i.e.FedRamp or IL5) limiting your agency's adoption of new mission-critical technology? If yes, how so?

COL David Lamy | AFC CIO

From the AFC CIO perspective, no. In addressing FedRamp identified requirements for applicable systems, applications, or cloud infrastructures FedRamp Authorizations are clear and concise, minimizing any ambiguities when it comes to implementing inherited Security Controls. However, the ability to accept reciprocity from FedRamp Provisional [Authorization to Operate] continues to be a hard sell to the Headquarters Department of the Army. Additionally, the federal authorization process provides qualitative and quantitative benefits to our organization's effort with regard to the adoption of mission-critical technologies and technologies in general.

Mark Curry | STE CFT

The FedRamp process is directly challenging the adoption of cloud computing by putting excessive strain on cyber resources at the service level. From the DoD perspective, we require at least an IL5 environment which requires [Defense Information Systems Agency (DISA)] certification. The agencies should do more to support the services with cyber assistance so that we can more effectively and expeditiously achieve DISA Provisional Authorization.

Tim Selph | N CFT

Not these specific processes. They are intended to standardize secure cloud services and have not limited our ability to leverage modern cloud technologies in coordination with our higher headquarters and operational units. However, the Army's traditional acquisition process does pose challenges in procuring and fielding emerging tactical communications technologies quickly enough to satisfy the demand from operational units. This frustration with the process can lead to units procuring technologies on their own, which may satisfy an immediate demand, but can pose lasting problems with integration and sustainment. While this friction remains, a recent expansion of acquisition authorities such as the Mid-Tier Acquisition pathway has given the Army more options to more quickly purchase and field mission-critical technologies.

How have continuing resolutions (CRs) or cyclical purchasing trends affected your agency's ability to procure new mission-critical technology?

COL David Lamy | AFC CIO

The impact of purchasing trends on our organization's balance between cybersecurity risks and our operational risks is observed primarily in personnel allocation — or lack thereof — to support incoming technologies. With the ever-increasing introduction of new technologies, an organization with limited resources or personnel may struggle to maintain the appropriate level of effort required for each product. Additionally, with new technologies comes a certain level of education — such as researching the new product and discerning potentially new processes to assess its security posture.

David Docimo | AFC G3/5/7

Programs that are transitioning through developmental to procurement activities, new starts, or programs that have increased funding requirements within the first quarter are adversely affected by continuing resolutions. The Army cannot disperse funds above the previous year's disbursement rates to maintain schedule. In general, under a short CRs, this affects only a half-dozen major programs each year. It places programs at risk of not meeting schedule for no other reason than funds are not available when needed. A second-order effect of continuing resolutions is that the Army now plans for them by adjusting program schedules to align with potential CRs. In a worst-case situation, this can unnecessarily extend programmatic schedules three months each year delaying the delivery of new capabilities to Soldiers over time.

Tim Selph | N CFT

Continuing resolutions are detrimental to the modernization and acquisition processes. For example, Army leadership testified in January 2022 that if a year-long CRs was passed, 71 Army programs would be affected because they are new starts, and 32 procurement programs would be delayed. These delays have a compounding effect because they must be prioritized in the next year, which further bumps these programs or projects. CRs also affect our ability to plan and execute large-scale modernization exercises such as Project Convergence, which are critical to the Army's modernization effort, including N-CFT-sponsored capabilities.

"Continuing resolutions are detrimental to the modernization and acquisition processes."

Tim Selph | Deputy Director, Network Cross-Functional Team

“Adequate funding to support IT infrastructure continues to be an issue.”

David Docimo | Army Futures Command Headquarters Directorate of Operations, Plans, and Experimentation and Assistant Chief of Staff

Are technology limitations creating risks for your agency? If yes, which technology limitations?

David Docimo | AFC G3/5/7

Adequate funding to support IT infrastructure continues to be an issue. The proposed migration to the cloud continues to be a challenge across the three domains in which we operate.

MAJ Brian Szczepanek | NGCV CFT

Yes. Many potential commercial technology solutions or services lack appreciation for the scale and scope our work requires. If a technology cannot quickly scale and integrate at scale through open source architecture standards, the costs will not provide commensurate benefits.

Mark Curry | STE CFT

Technologies such as AI add risk to projects as they are complicated, slow to develop, and need large amounts of data to optimize. The translation of human elements to machine learning also carries significant costs and expertise. We continue to collaborate with industry and government partners to better understand cutting-edge capabilities, applications of emerging technologies, and how we can best deliver these concepts to the warfighter.

Bridgett Siter | SL CFT

There is risk in the mindset of thinking that once a technology reaches a certain point, the risk will go away. There is a saying in the operational force, “the threat always gets a vote in the fight.” In this case, the pace of technology means that peer competitors are developing capabilities that keep pace with the United States — even if they fail to use those technologies appropriately, as Russia has so aptly demonstrated.

When choosing new technologies to support the mission, how does your agency balance its technology risk (i.e. cyber risks) with your mission's operational risks (i.e. do you have the capability to keep pace with threats and achieve the desired outcome)?

COL David Lamy | AFC CIO

The increasing tempo and complexities of emerging technologies present an issue with regard to an organization's ability to keep pace. Similar to the answer in question three, there's a myriad of pre-requisite information and knowledge that would be required to conduct the security assessments and analysis per technology and the specific operational environment that may not be viable due to resources and personnel constraints. [Army Futures Command Headquarters] currently utilizes the [Research Development, Test and Evaluation (RDT&E) Defense Research Engineering Network (DREN)/ Secret Defense Research Engineering Network (SDREN)] to test and generate artifacts to support moving new and existing technology forward to the Operational Platforms through test and evaluation.

Bridgett Siter | SL CFT

The SL-CFT has a threat cell that continually updates its peer threat assessment by pulling information from multiple sources. That cell provides leaders with insights to mitigate operational risk. Additionally, the SL-CFT also accounts for industrial and funding risks. Furthermore, by incorporating assessment from the Army's combat formation Capability Managers, it enables a deliberate approach to decision making. The SL-CFT staff uses a modified version of the military decision-making process to incorporate all data and enable sound decision-making by its leadership.

Tim Selph | N CFT

The Army uses Capability Sets to execute an incremental network modernization approach across the force while keeping pace with technology advancements and emerging threats. This strategy leverages commercial solutions informed by synchronized Soldier touchpoints, experiments, and developmental and operational tests, including frequent cyber security assessments. Going forward, we are adapting our architecture and encryption to keep pace with future technology, including Zero Trust and multi-level security approaches.

"The increasing tempo and complexities of emerging technologies present an issue with regard to an organization's ability to keep pace."

COL David Lamy | Chief Information Officer, Army Futures Command Headquarters

What programs have been the most helpful for adopting new technology, and where have those programs still come up short in servicing your mission requirements?

COL David Lamy | AFC CIO

The Army IT Acquisitions program is done well through [Computer Hardware, Enterprise Software, and Solutions (CHESS)] for procurement of [commercial off-the-shelf] hardware and software. However, after the IT is acquired, the Army falls short in the approval and implementation of IT hardware and software. This stems from many points, however, the lack of availability of a complete list of approved hardware and software products at the lowest levels is a strong point of contention. The [Department of Defense Information Network (DoDIN) Approved Products List (APL)] is used in conjunction with CHESS, however, the DoDIN APL includes mostly hardware requests. One potential solution is the creation of a single point where users can view a list of hardware and software that is readily available for use, available for use with a request for approval, or still requires assessment and authorization for use. The DoD in general is slow in providing full transparency of systems technologies that may have cybersecurity implications — such as AI — and the Army falls short in providing cybersecurity tools to the [DoD Cyber Workforce Framework (DCWF)] and the training to use the tools.

Jim Thomson | FVL CFT

The most important signature effort [for FVL CFT] is the modular open system approach — or MOSA. The FVL MOSA establishes standards and common interfaces around a digital backbone that allows the rapid on-/off-boarding of hardware and software without the need to go through the platform's original equipment manufacturer — or OEM. This allows for the rapid integration of technologies in order to maintain pace and provide overmatch against adversary threat systems.

Mark Curry | STE CFT

The use of the Small Business Innovation Research — or SBIR — program has been helpful in identifying and acquiring new technologies. The STE CFT has been able to fund three SBIRs through Army Futures Command to address Adaptive Training or Intelligent Tutoring and Network Data Compression.

MAJ Brian Szczepanek | NGCV CFT

Pre-materiel solution analysis technical demonstrations and objective performance experiments have been crucial in our assessment of new technology and refinement of requirements. Field events focused on areas such as autonomy or protection are examples of linking new technologies to our platforms while larger experiments like Project Convergence enable us to understand how well new technologies will integrate across the wider Army operational spectrum.

How can agencies collaborate with industry to shorten adoption times, facilitate faster processes, and maximize mission-critical technology?

COL David Lamy | AFC CIO

Through the establishment of partnerships, full utilization of working with industry programs outside of the acquisition process. There is a need for more collaboration with industry, joint partners, and other federal agencies from a cybersecurity perspective. Also, make sure that the Cybersecurity Maturity Model Certification (CMMC) is understood, adequately implemented, and mandated.

Bridgett Siter | SL CFT

Agencies that are serious about shortening adoption times, facilitating faster processes, and maximizing mission-critical technology need to (1) have/listen to experts on their staff who understand why a requirement is a requirement. Those experts cannot be just someone who was in the Army for a couple of years. (2) Attend and ask for industry days. (3) Ask for meetings with CFTs and requirements developers to understand why a requirement is being developed. (4) Schedule briefs with requirements developers, Science and technology leads, and the Acquisition leads on CFTs.

MAJ Brian Szczepanek | NGCV CFT

Shifting from largely transactional relationships to more collaborative ones is critical. Products are not always solutions. Identify where and why Army is late to technology users, whether the application of new technology reduces or adds to the cognitive load of the user, and how efficiently — low integration, training, operating, maintaining overhead — the technology reduces the costs of sharing information. There is a need to develop a common perspective on the problem to solve.

Tim Selph | N CFT

Given the rapid evolution of network technology in the commercial sector, the Army is using a recurring Technology Exchange Meeting — or TEM — process to influence industry internal [research and development] efforts, and has awarded numerous prototyping contracts that are informing future capabilities. Odd-numbered TEMs are informational; even-numbered TEMs solicit whitepapers for potential prototyping contracts. Based on Network CFT and other stakeholders' analysis of the whitepapers, the Army then issues select invitations for vendors to execute technology demonstrations prior to down-selecting for contract awards. This process has fostered transparency with industry in order to align their investments to mission-critical technologies for future Capability Sets.

"Shifting from largely transactional relationships to more collaborative ones is critical."

MAJ Brian Szczepanek | Deputy Chief of Operations, Next Generation Combat Vehicle Cross-Functional Team

INDUSTRY PERSPECTIVE

JOE BALCHUNE

Vice President, Federal Markets
at Motorola Solutions Inc.

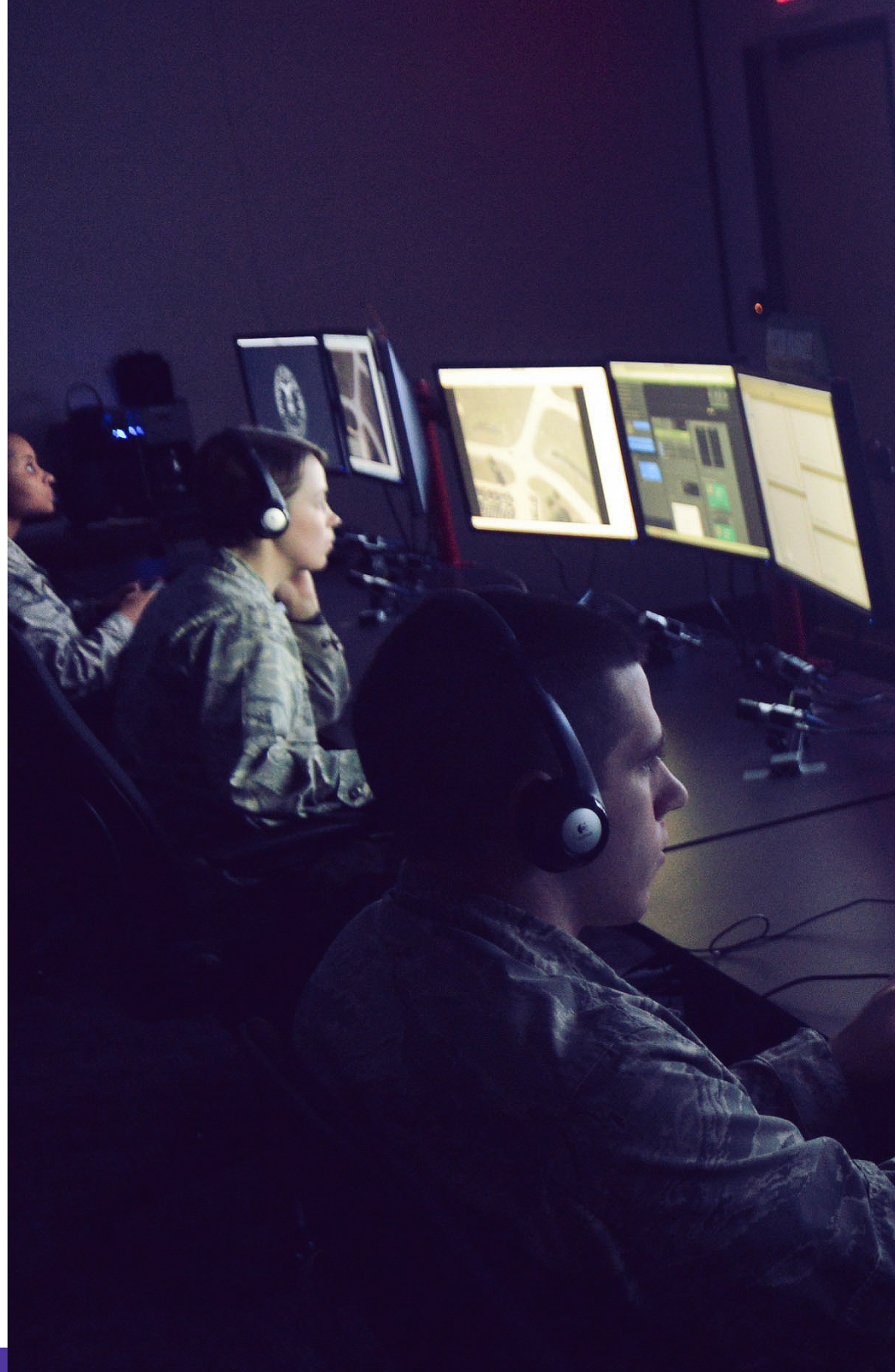
How are technology providers helping federal agencies gain greater control over their digital and IT transformation journey?

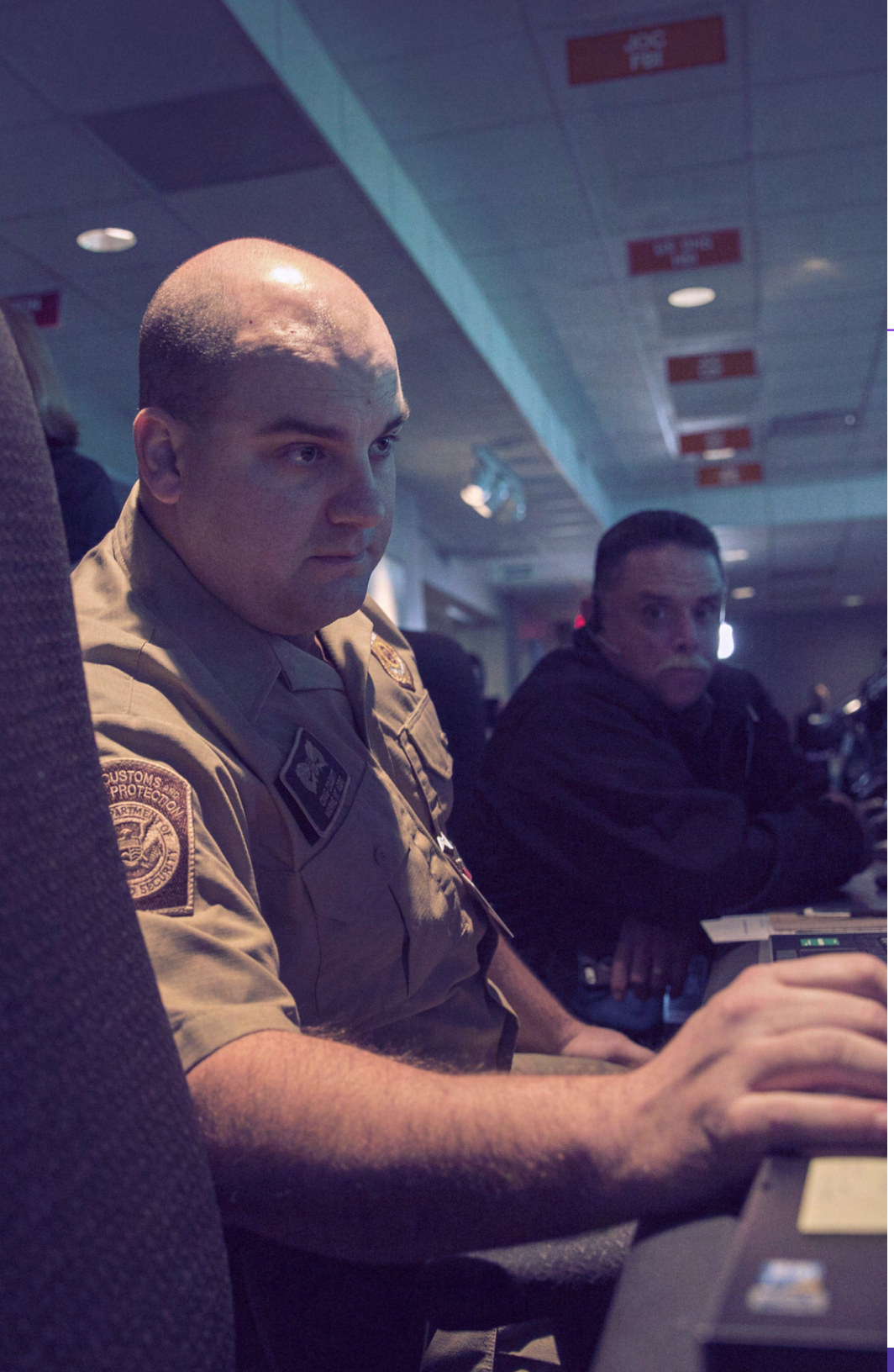
Joe Balchune | Vice President

Most technology companies selling in the US federal government market understand that their customers want greater control over their IT and communications transformation. That means more choice in payment and deployment models, such as buying solutions on an as-a-service basis. And it means relying more on open systems architecture that can be hosted in the cloud, on prem, or a hybrid configuration. Yet, knowing this and actually delivering on it, are often two separate things and some companies are finding more success in navigating this path than others.

At Motorola Solutions, we're developing mission-critical voice, video, and data capabilities for both on-premise and cloud-based environments that empower customers with more control over what they buy and how they use it.

That starts with meeting and, often exceeding, security requirements across multiple classification levels. It includes offering modular solutions that allow customers to purchase only what they need, when they need it, while making it easy to integrate technology both across our portfolio and with other systems and data sources. We're also focused on helping our customers manage technology in a way that works best for them, given their internal resources, with services that support their people, processes, and policies.





How are technology providers meeting government security and operational requirements to speed their customers' time from purchase to deployment?

Joe Balchune | Vice President

I can only speak for Motorola Solutions but I can tell you, we're working hard to ensure all mission-critical technology requirements are met as early in the product lifecycle as possible to help speed adoption and utilization. There are a variety of strategies we've put in place to support this approach. As an example, the work we do collaboratively with government agencies in both their programs, such as NSA's Commercial Solutions for Classified (CSfC), and their laboratories, like DISA's Joint Interoperability Test Command (JITC) for certification, validation, and continuous testing is an important part of our process. Internally, we invest in IT systems we own and manage to deliver shared services. One example of success in that area is our Cybersecurity Maturity Model Certification (CMMC). We also operate a secure design facility to develop security capabilities such as encryption, authentication, credentialing, and access control for Zero Trust and multi-level security needs. Some of the strategic acquisitions our business has made over the last several years include companies that have served as a FedRAMP 3PAO or have already achieved FedRAMP. In addition, we are in the process of obtaining FedRAMP High on our cloud environment, which means that agencies that sponsor our mission-critical technologies for authorization can reap the benefits of a platform with security baseline controls already in place. We're extremely dedicated to finding greater efficiencies that improve our customers' time from purchase to deployment.

FINAL CONSIDERATIONS

Rapidly acquiring **mission-critical technologies** is vital not only for the protection of America's collective assets but also for keeping pace with potential adversaries. While an emphasis on cybersecurity is a primary consideration, lengthy review processes can also delay the adoption of these mission-critical technologies. As mentioned above, the barriers to adopting mission-critical technology can create new, operational risks that limit our nation's ability to keep pace with threats and achieve mission success. Therefore, how mission-critical technologies are acquired is central to managing the balance between cybersecurity risks and operational risks. Partnering with the industry partner can be pivotal in acquiring mission-critical technologies without compromising cybersecurity.

ABOUT US

Government Business Council

As GovExec's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research analysis.

For more information:

research@govexec.com

www.govexec.com/insights

MOTOROLA SOLUTIONS

Motorola Solutions is a global leader in public safety and enterprise security. Our solutions in land mobile radio communications, video security & access control, and command center software, bolstered by managed & support services, create an integrated technology ecosystem to help make communities safer and businesses stay productive and secure. At Motorola Solutions, we're ushering in a new era in public safety and security.

Learn more at:

www.motorolasolutions.com


Government
Business
Council