

PRINCIPLES OF

Digital Modernization:

A LOOK AT DOD

INSIDE:

- The Army's 2023 IT Modernization Plan 3
- Components of Digital Modernization 6
- IT-as-a-Service: Army BYOD Program 11

SPONSORED BY



From the writer's desk



Kate Macri, Deputy Editor

The Pentagon's Digital Modernization Progress

The Pentagon's digital modernization journey is a fantastic example of the myriad nuances and intricacies associated with updating legacy IT infrastructure for the 21st century, especially when handling classified and unclassified data.

Artificial intelligence (AI), bring-your-own-device (BYOD)

programs, DevSecOps and zero trust can help the Defense Department and other federal agencies revamp IT, but efficient modernization often comes down to resources and relationships. Industry and government are working together to find the right recipe for digital modernization while balancing concerns around IT bloat and workforce retention. 🌟



Table of Contents



Sarah Sybert,
Staff Writer



Anastasia Obis,
Staff Writer

ARTICLE

Army CIO Releases Updated Data, Cloud Plans

The service is moving away from being network focused to being data centric.

BY SARAH SYBERT

INFOGRAPHIC

Components of Digital Modernization

Effective digital modernization strategies require strong partnerships with industry, iterative solutions, an enterprise approach and a little help from artificial intelligence.

PARTNER INTERVIEW

How to Develop a Savvy Digital Modernization Strategy

Policy-oriented tools such as TMF and zero trust can help federal agencies prioritize digital modernization efforts.

Steve Hull, Executive Vice President for Cyber Operations, Leidos

ARTICLE

Army Scales Up Its Bring-Your-Own-Device Program to More Soldiers

BYOD program will let soldiers and DOD civilians securely access government systems through their personal devices.

BY ANASTASIA OBIS



Army CIO Releases Updated Data, Cloud Plans

The service is moving away from being network focused to being data centric.

BY SARAH SYBERT

The U.S. Army’s new cloud and data plans underpin the service’s vision of a data-centric future, Army CIO Raj Iyer said during an AUSA media roundtable in Washington D.C.

“Across the Army, at echelon, all the commands are now taking that data centric-objective and then looking at how they need to modify and realign each of their own initiatives and programs to make sure they align with that secretary’s priority,” Iyer said.

The updated plan reprioritizes the service’s efforts on the enterprise side. Iyer said that the Army plans to aggressively cut down the number of data centers the service owns, aiming to only have five enduring data centers.

“Then, we’re going to link that up with a commercial cloud ... what we’re calling a hybrid-cloud architecture ... and that is our ‘to-do’ thing for fiscal year 2023,” Iyer added. “When we do that, we’re now going to have a seamless environment between those five private clouds and the commercial cloud, and



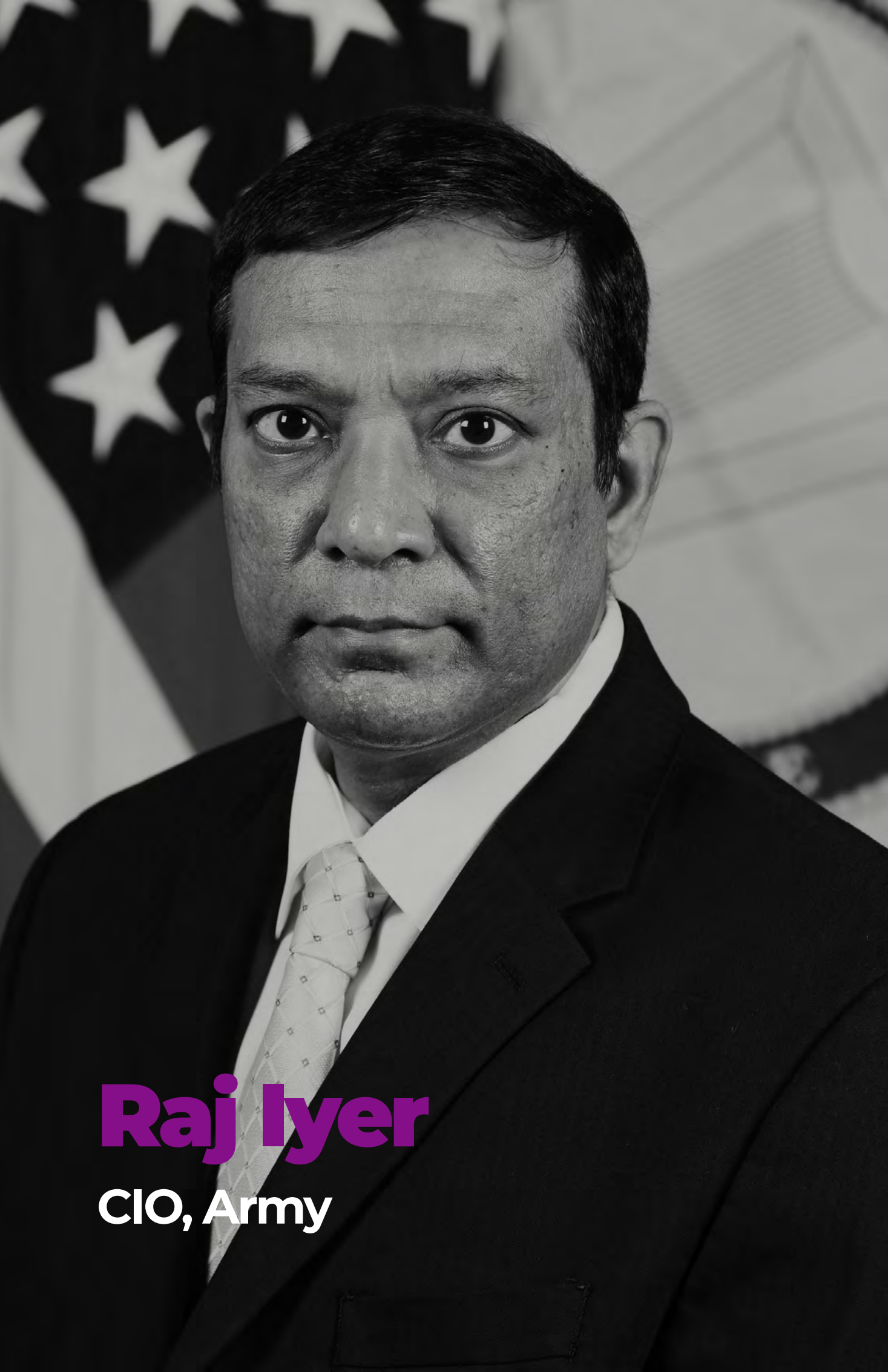
we can now seamlessly move data between the two.”

Moving applications to the cloud will become even more critical. In fiscal year 2022, the service moved approximately 100 applications to the cloud, but the Army still has a long way to go. In the new year, Iyer said the Army will conduct “keep or kill” analysis of systems to consolidate before moving to the cloud and has already killed 66 business applications this year alone. In fiscal year 2023, the Army committed to another 103 systems to sunset.

“Between now and fiscal years 2025 to 2026, we’re looking at a 50% reduction in the number of applications and systems that the army owns,” Iyer said.

In support of those migration requirements comes a new enterprise contract vehicle called the Enterprise Application Migration and Modernization (EAMM) contract — a \$1 billion multi-award, multi-vendor IDIQ.

“We’re going to establish that here in the second or third quarter of fiscal year 2023,” Iyer said. “This is going to become the easy button for the Army to



Raj Iyer
CIO, Army

actually move to the cloud.”

Zero trust will underpin Army’s cloud and data modernization.

“What we’re doing differently is we’re now establishing an integrated program office for zero trust ... [to] align all these efforts under a single command and control,” Iyer said.

The new program office will ensure a unified, single reference architecture and integrate best-of-breed commercial tools. In terms of implementation, the office will focus on capturing all the dependencies and aligning funding to meet these priorities. As part of the Army’s zero trust journey, the service will work to fully build out its identity, credential and access management (ICAM).

“ICAM is going to be the big implementation for this year,” Iyer said. “The other piece is, through the cloud, we’re going to implement secure access service edge (SASE).”

The Army will hone in on operational technology as it continues to secure its critical cyber infrastructure. The service was awarded \$15 million from the Technology Modernization Fund (TMF) to enable attack sensing and warning (AS&W) and vulnerability assessment cyber capabilities and establish a security operations-as-a-service framework that ensures cyber defenders can monitor, respond to and remediate cyber threats.

“With this funding from the White House, we are prioritizing our industrial base and working with our industrial base partners, really censoring our operation technology networks, and then be able to remediate,” Iyer said.

The Army will also prioritize its data fabric to integrate various data into a common operating picture.

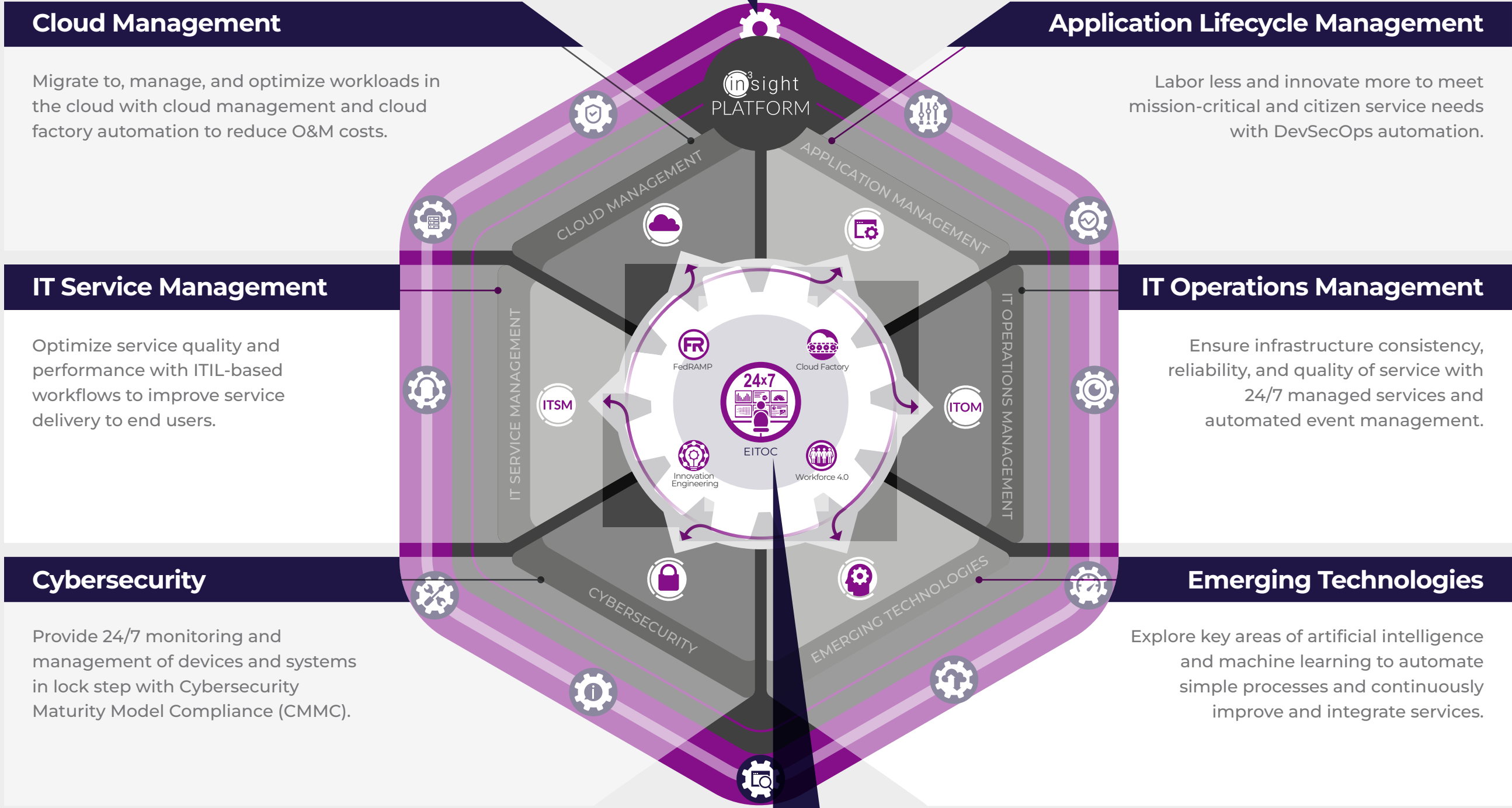
“The Army really is in a very mature place when it comes to being able to synthesize data,” Iyer said. “There’s still a long way to go in terms of greater integration with our allied and coalition partners. So one of the other priorities for us this year in fiscal year 2023 is a mission-partner environment. ... We’ll move away from being network focused to being data centric.” 🌟

“The Army really is in a very mature place when it comes to being able to synthesize data. There’s still a long way to go in terms of greater integration with our allied and coalition partners. So one of the other priorities for us this year in fiscal year 2023 is a mission partner environment. ... We’ll move away from being network focused to being data centric.”

—Raj Iyer, CIO, Army

As agencies explore as-a-service models for digital modernization, they can leverage documented frameworks to guide stakeholder buy-in and ultimately planning and execution.

**Platform Delivery of IT as a Service:
A Framework for Success**



Cloud Management

Migrate to, manage, and optimize workloads in the cloud with cloud management and cloud factory automation to reduce O&M costs.

Application Lifecycle Management

Labor less and innovate more to meet mission-critical and citizen service needs with DevSecOps automation.

IT Service Management

Optimize service quality and performance with ITIL-based workflows to improve service delivery to end users.

IT Operations Management

Ensure infrastructure consistency, reliability, and quality of service with 24/7 managed services and automated event management.

Cybersecurity

Provide 24/7 monitoring and management of devices and systems in lock step with Cybersecurity Maturity Model Compliance (CMMC).

Emerging Technologies

Explore key areas of artificial intelligence and machine learning to automate simple processes and continuously improve and integrate services.


Enterprise IT Operations Center



How to Develop a Savvy Digital Modernization Strategy

Policy-oriented tools such as TMF and zero trust can help federal agencies prioritize digital modernization efforts.

Steve Hull, EVP & Operations Manager, Enterprise & Cyber Solutions

 **What policy priorities should federal IT leaders keep in mind when developing digital modernization strategies?**

Hull If you look at it from a government policy standpoint, federal IT leaders need to understand the goals of the Technology Modernization Fund (TMF): reducing technical debt while modernizing digital infrastructure and reducing vendor lock-in while democratizing data. They should also be aware of the 21st Century Integrated Digital Experience Act (IDEA), which requires all executive branch agencies to modernize websites and digital services and improve the overall digital experience on federal public websites.

Beyond policy, zero trust is especially important for IT leaders. Not many people understand what zero trust is — it's not something that you purchase, it's a cybersecurity methodology and architecture.

In addition, the shift to purchasing IT as an operating



expense rather than a capital expenditure — especially when it comes to noncapital purchases like cloud and as-a-service models — remains central to modernization.

What are the biggest barriers to digital modernization in government right now, and how do you advise overcoming them?

Hull Many of the barriers to digital modernization are due to the pace of the acquisition process. The government is centered around requests for proposals (RFP). This means there is a long process before an agency selects a provider or service, and its decision is often protested, which can delay a contract award. Another challenge is that an agency might piece up services to many different integrators, as well as medium and small businesses. This becomes even more difficult when there are issues. Aggregating requirements into larger RFPs and contracts could help the federal government streamline the process and overcome these issues.

The size of the enterprise can be another barrier. For example, a large service branch within the Defense Department (DOD) may have a massive

program with disparate IT, making it difficult to modernize and measure improvement. With such a hard problem to solve, agencies will also have many different projects in flight and must understand how to engineer all the implementations with dependencies in a concerted fashion. Finally, budget continues to be a challenge because modernization is expensive.

How can defense and civilian agencies work on closing the workforce gap and upskill current workers to meet digital modernization goals?

Hull The talent shortage is a hard problem. As the country is shifting to remote work in many industries, the government also needs to adapt with more flexible working arrangements to attract and retain talent. There are challenges with classified work being done remotely, but I've seen successful instances of doing development work on the unclassified side and moving it to the classified side.

Government and federal contractors are also competing with commercial companies that attract the same candidates. These companies can offer flexible and fully remote work. The government mission attracts many employees, but the government needs to think about how to make the jobs

“Aggregating requirements into larger RFPs and contracts could help the federal government streamline [the digital modernization] process.”

Steve Hull, EVP & Operations Manager, Enterprise & Cyber Solutions

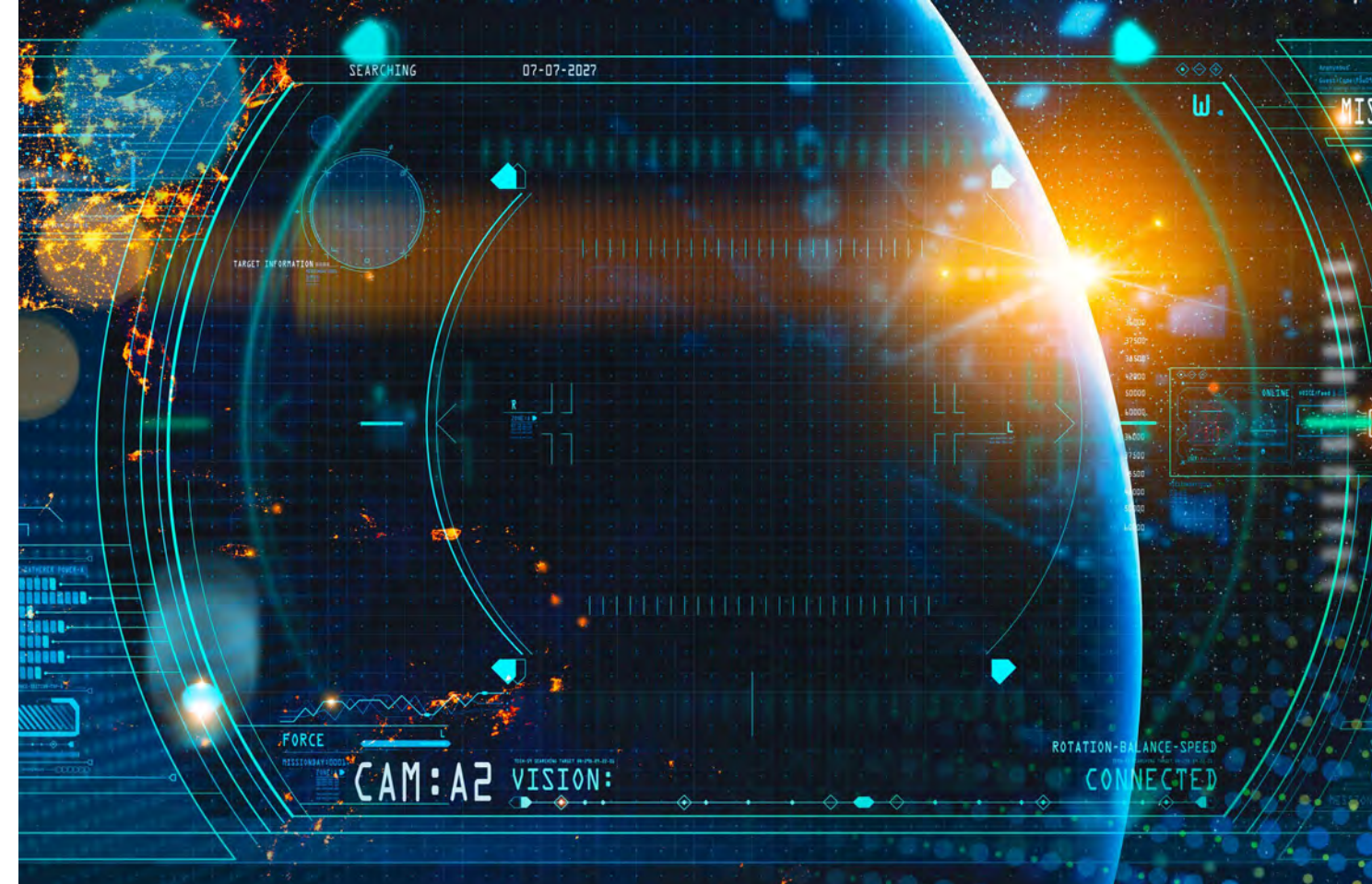
even more appealing. Upskilling is key to growth and helps maintain an agile workforce. Government will need to plan deliberate upskilling programs to ensure employees can support IT systems through modernization.

Defense and civilian agencies should consider widening the aperture of the candidate pool. For example, sometimes a degree isn't required for IT work. In cyber especially, employees can train and don't need a four-year degree to do so. Both the government and federal contractors need to work more closely with high schools and colleges, particularly in STEM programs, to help students understand the skill sets needed and help the administrators drive the curriculum so that students are prepared when they join the workforce.

How can new infrastructure modernization strategies, such as enterprise IT-as-a-service and “bring-your-own-device” (BYOD), help defense and civilian agencies accelerate digital modernization? What are some pitfalls to watch out for?


Hull Historically, federal agencies wanted a close hold on their IT organizations with everything on premise. Then as Microsoft 365 rolled out its cloud-based service, customers found that it wasn't terrible — they may not control everything on premise, but they also do not have the high capital expenses. They're using an as-a-service model, and instead of spending \$1 billion on hardware, they are only spending on what they consume.

Bring your own device (BYOD) is also interesting because it allows employees to use the device that they want to work on, letting them be more comfortable in their environment. It also makes it easier on the enterprise and eliminates the need to stock and manage thousands of computers and phones. However, BYOD often faces security restriction issues. What an employee does for work sometimes can't traverse the barriers of a personal device, so that customization for work purposes may not always be possible. Trying to architect for these more secure environments is an ongoing effort.



What roles do artificial intelligence (AI) tools like algorithms and scripts play in modernization?

Hull Speed. For example, the Navy's networks have tens of thousands of network devices. If updates can be scripted to go out at the same time to all devices, that's a game changer. AI also does a good job of “raising the smartness” of everyone; it can point an analyst to more interesting events so the analyst does not have to look at log after log — training them over time to spot things they haven't seen before. For instance, AI can recognize risk patterns where adversaries have been trying to trick algorithms. With that information, we can update the algorithms and make them smarter so that adversaries can't do those things easily.

Digital twins are another application of AI where an environment is put into a model-based systems engineering app. With a digital twin, changes can be made to the model first to make sure nothing breaks down the line, rather than having a massive test environment. This is how we need to think about true modernization moving forward. 



Secure technology, at scale and speed

At Leidos, we drive digital transformation initiatives with meticulous planning, technology disruption, and collaborative execution. Count on us to design and deliver resilient cloud, network, and application infrastructure that ensures end-user effectiveness today and automates the defense of mission-critical systems and data for threats yet faced.

Learn how we're applying secure technology, at scale and speed, in missions of global importance.

leidos.com/capabilities

Army Scales Up Its Bring-Your-Own-Device Program to More Soldiers

BYOD program will let soldiers and DOD civilians securely access government systems through their personal devices.

BY ANASTASIA OBIS

The Army is preparing to roll out its bring-your-own-device program to about 20,000 soldiers and civilian employees. It's the next step in the service's initiative as part of a larger Defense Department effort to allow service members and civilians to work on their phones and home computers.

Lt. Gen. John Morrison, the Army's deputy chief of staff, G-6, spoke about the program during a CyberCast interview at the Association U.S. Army Annual Meeting & Exposition. He explained the primary focus for Army officials is on analyzing user experience and security.

The Army has been testing technologies for the BYOD program for over a year, allowing the service to build a foundation for the program's strategy and carry the successes of the initial rollout into the next stage. The program had an immediate operational impact, specifically with its National Guard partners. It also proved to have sufficient security, Army officials said.



“The ability to support operations, that usability from a user perspective, a capability that they like to use, and then having that security wrapper around it — all three of those we have rolled over into this next instantiation of the pilot, which is far broader than what we did the first time,” Morrison said.

Throughout multiple testing stages of the program, cybersecurity



Lt. Gen. John Morrison

Deputy Chief of Staff,
G-6, Army

remained the primary component and key element for the Army.

“We really have sort of inside our Army flipped the paradigm of how we look at the problems. Instead of cybersecurity being something we bolt on at the end, that’s really not a good way to approach it. We bake it in on the front end,” Morrison said during the CyberCast interview.

“With bring your own device, that’s exactly what we’ve done. And the technical instantiation is, while there’s an application that resides on your phone, none of the data does. It’s still all resident in the cloud with the appropriate defensive cyber watch over the top of it.”

Meanwhile, the Army is executing a Google Workspace pilot, one of the Army’s multiple IT modernization efforts, along with the BYOD program. The part of building out a cloud at the impact level 4 is over and the Army is currently evaluating how this effort fits into its future.

“I do have to emphasize that it is a pilot. It’s a fairly robust pilot,” Morrison said. “But as of about two weeks ago, all new accessions coming into the Army, we were issuing Google workspace accounts to include email, so that’s what they just start on. And then we’ll eventually populate most of the training base.” ❁

“Instead of cybersecurity being something we bolt on at the end, that’s really not a good way to approach it. We bake it in on the front end. With bring your own device, that’s exactly what we’ve done.”

Lt. Gen. John Morrison, Deputy Chief of Staff, G-6, Army