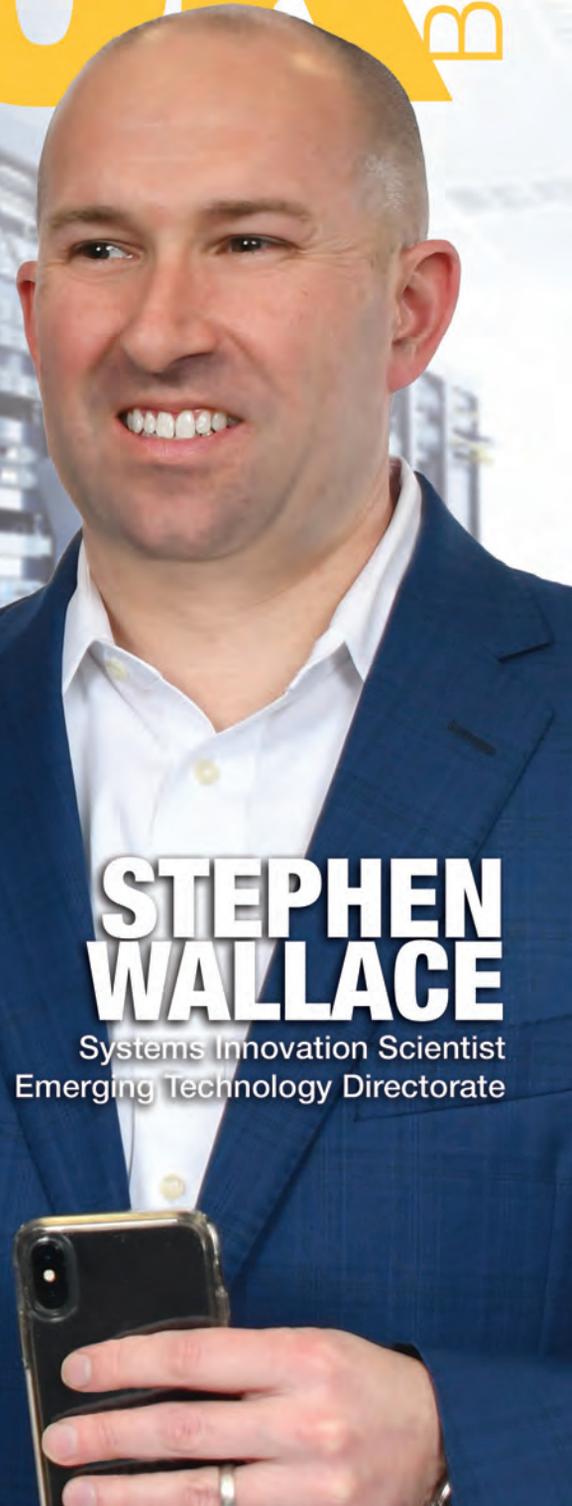


SUMMER 2020 DISA LOOK BOOK

EDITION

Emerging Technology



STEPHEN WALLACE

Systems Innovation Scientist
Emerging Technology Directorate

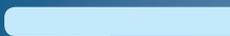
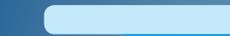
- Blockchain
- Ecosystem Automation
- JEDI
- Desktop Convergence
- DevSecOps
- Artificial Intelligence
- Zero Trust



Lk
Bk



EMERGING TECHNOLOGY

-  **Blockchain**
-  **Ecosystem Automation**
-  **JEDI**
-  **Desktop Convergence**
-  **DevSecOps**
-  **Artificial Intelligence**
-  **Zero Trust**

SUMMER |

LOOKBOOK |



Sherri Sokol

BLOCKCHAIN
LEAD
EMERGING
TECHNOLOGY
DIRECTORATE



BLOCKCHAIN

Infrastructure-as-a-Service

Blockchain Infrastructure-as-a-Service is a preview version of a potential service offering to provide a Department of Defense-accredited, scalable method of standing up business networks. The Emerging Technology Directorate and the Mainframe Line of Business partner together on this effort to enable DoD organizations to breakdown silos of information and use those data as an asset, moving to a more connected and automated way of doing business while maintaining a high level of security. BaaS will also streamline the path to production blockchain systems in the future.

Blockchains are distributed digital ledger systems. They enable the user community to record transactions in a shared ledger, so that once published, transactions cannot be changed without the community knowing.

Many DoD business networks still use paper-based or manual systems to record information and manage records. Even when the data are in digital form, gathered via automated methods, they are often stored in disparate systems that do not talk to each other.

In this current state, the task of locating, verifying and tracking information and assets can be very difficult, labor intensive and time consuming. To audit, individuals must piece together data manually to determine end-to-end processes and sources of issues. Additionally, the potential for inaccurate and/or incomplete data leads to untrusted data, which compromises the ability to gain insights that are actionable

and timely. The data cannot be used as a strategic asset.

BaaS provides a solution to these issues by enabling a shared system for recording the transaction's history. By incorporating executable code via mission partner-distributed applications, smart automation can occur based on the data captured in the transactions. Information is (selectively) shared among

Justin Sollenberger

SYSTEM
SUPPORT
BRANCH
CHIEF,
MAINFRAME
LINE OF
BUSINESS



participants, enabling everyone to gain insights, accelerate informed decision-making, reduce the friction and cost in data exchanges and add new network members and data processes/workflows with relative ease. Additionally, when blockchain is combined with other emerging technologies (e.g., artificial intelligence, machine learning, robotic process automation and internet of things), it can become a force multiplier.

The preview BaaS offering provides hosting services for Hyperledger blockchain networks through which operators are provided with support and management tools. These tools include a simplified software development kit, code patterns, tutorials and a management console. The solution distributes images of the blockchain platform in containers; which are managed, secured and centrally orchestrated. Mission partners can use BaaS to deploy their separately-built and accredited, use-case-specific, distributed applications, which write to and read from the distributed ledger. Mission partners are then responsible

for the operation of their own distributed application instances.

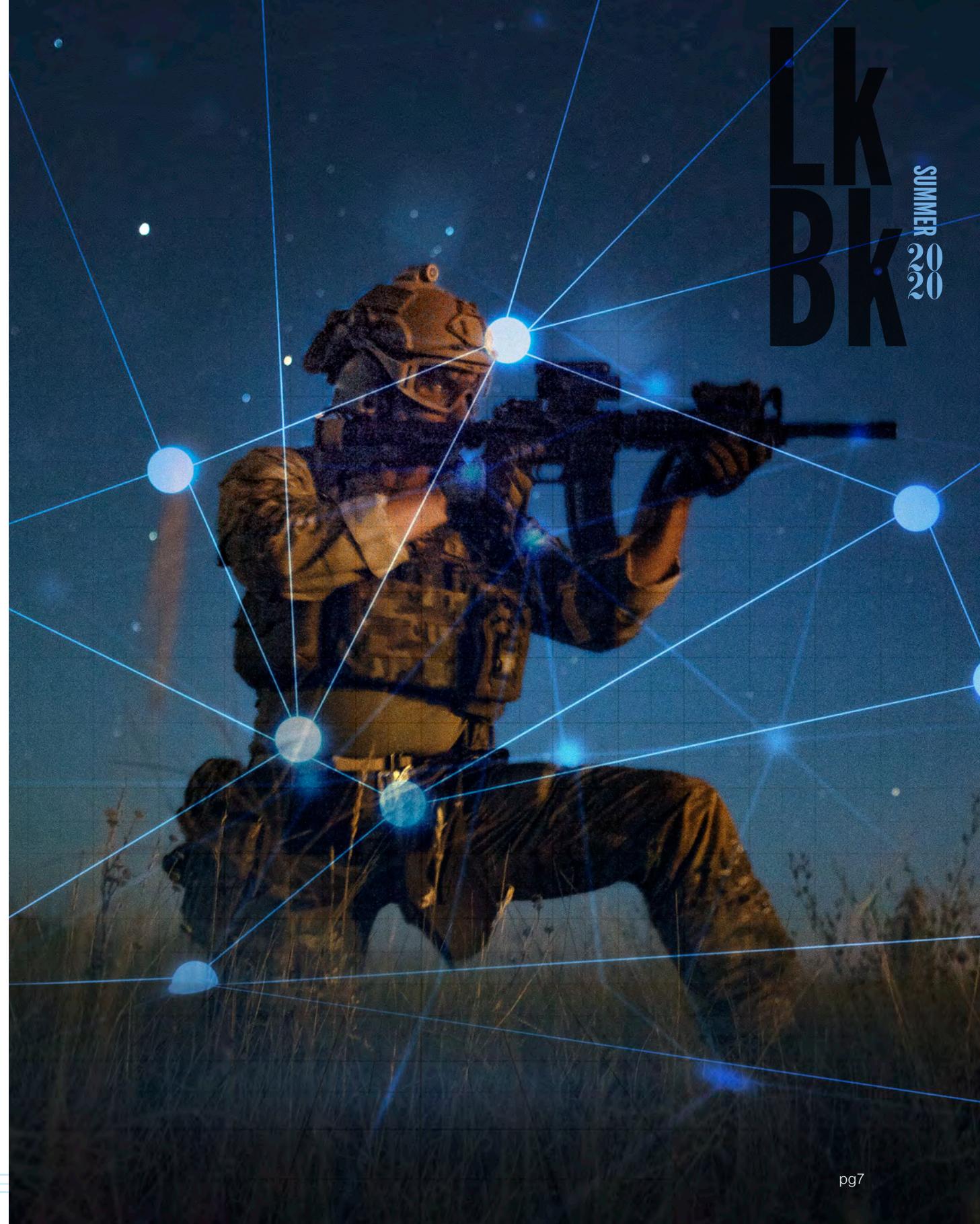
With DoD-accredited BaaS, mission partners have a platform where they can implement capabilities that align to and support DoD's goal to strengthen the security and resilience of networks and systems that contribute to current and future United States military advantages. *DoD's Digital Modernization Strategy* specifically highlights blockchain as a technology offering of promise to DoD. Its inherent factors — including transparency, tamper resistance, cryptographic data structure and resiliency — denote its potential as a cybersecurity shield, which also speaks to DISA's strategic objectives of modernizing the infrastructure and strengthening cybersecurity.

BaaS offers another innovation when it comes to its pricing model. While the exact cost of providing BaaS has yet to be determined, since BaaS is only in preview, the offering fits with the vision of moving to a container-based pricing model for mainframe. This is the final piece of the puzzle to open the door for hosting smaller workloads for mission partners, which increases the ways DISA can enable them to achieve their mission sets.

BaaS is also part of a broader modernization effort that enables innovative services on a mainframe. It takes advantage of the enterprise mainframe computing power and expertise DISA already offers and incorporates emerging technologies and approaches.

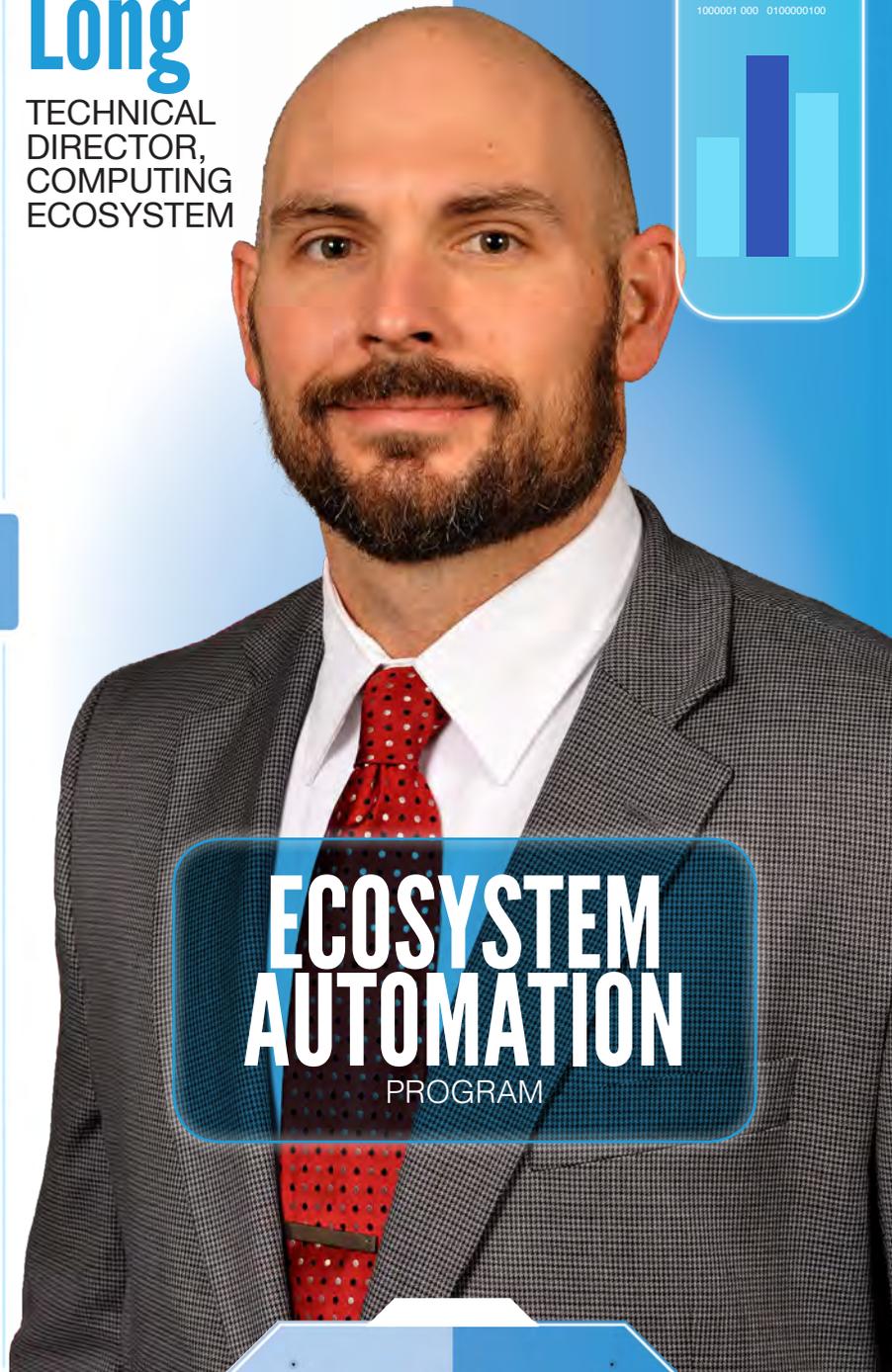
BaaS opens up DISA's enterprise backbone for a new way of doing business while also widening the kinds of workloads able to be hosted on a mainframe.

Bk
CH



Nathan Long

TECHNICAL DIRECTOR, COMPUTING ECOSYSTEM



ECOSYSTEM AUTOMATION PROGRAM



The Ecosystem Automation Program is the latest effort to continuously improve service support to mission partners. It leverages an orchestration tool to automate workflows for repeatable, and often time consuming, technical and procedural tasks that cross various lines-of-business. What used to rely on manual “hand-offs” from one system, technician or line-of-business to another, now moves through an automated workflow that enables ecosystem technicians self-service access across lines-of-business.

The payoff is a significant improvement in the speed of servicing mission partner needs.

One example is ad hoc scanning. By automating the ability to initiate an ad hoc scan through the Assured Compliance Assessment Solution, or ACAS, from the Enterprise Security Posture System, DISA has saved on average 24 hours per scan. There are on average 3,000 ad hoc scans created every month.

This is just one of numerous improvements. Ecosystem has demonstrated significant time savings through automating functions in remediation task management, tracking Host Based Security System compliance and assigning internet protocol addresses to various networks.

DISA’s move to establish an enterprise ecosystem a few years ago was an important shift in removing locationbased stovepipes, and positioned DISA as an enterprise-class computing service provider. Automation further

provides mission partners an accelerated deployment of their servers into DISA’s secure ecosystem-managed environment.

The process starts by gathering all required system information up front and inputting data into an orchestrated workflow that automates the necessary tasks across multiple lines-of-business. This upfront information gathering ensures that all aspects of a project can be incorporated from the start, ultimately leading to quicker system deployment with fewer issues during the build process.

In an ever-changing cyber environment, the ability to apply patches and mitigate findings becomes more and more important. The use of automation to standardize patch deployment enables ecosystem to report and mitigate security findings in a fraction of the time, significantly reducing the likelihood of human error.

The future of automation is one of vast possibilities and endless use cases. Ecosystem is currently using a variety of toolsets to build and deploy automation systems. Future plans aim to consolidate automation onto a common platform capable of integrating with the various technology platforms and business tools. This common platform will allow DISA to publish playbooks and establish a repository for others around the agency to leverage for similar tasks. It will also allow ecosystem to eliminate the manual effort required to document changes and incidents.



**Casey
Hurt**

TECHNICAL
DIRECTOR,
CLOUD
COMPUTING
PROGRAM
OFFICE

**JOINT ENTERPRISE
DEFENSE
INFRASTRUCTURE**

Cloud

SUMMER |

LOOKBOOK |

JOINT ENTERPRISE DEFENSE INFRASTRUCTURE CLOUD

The Joint Enterprise Defense Infrastructure Cloud will provide DoD with a secure and extensible cloud environment that spans from the homefront to the global tactical edge, as well as the ability to rapidly access computing and storage capacity to address warfighting challenges at the speed of relevance. The JEDI Cloud will play an integral role in supporting warfighters to maintain DoD military advantage.

JEDI is a \$10 billion pathfinder program, one of the largest non-weapon acquisitions in DoD's history.

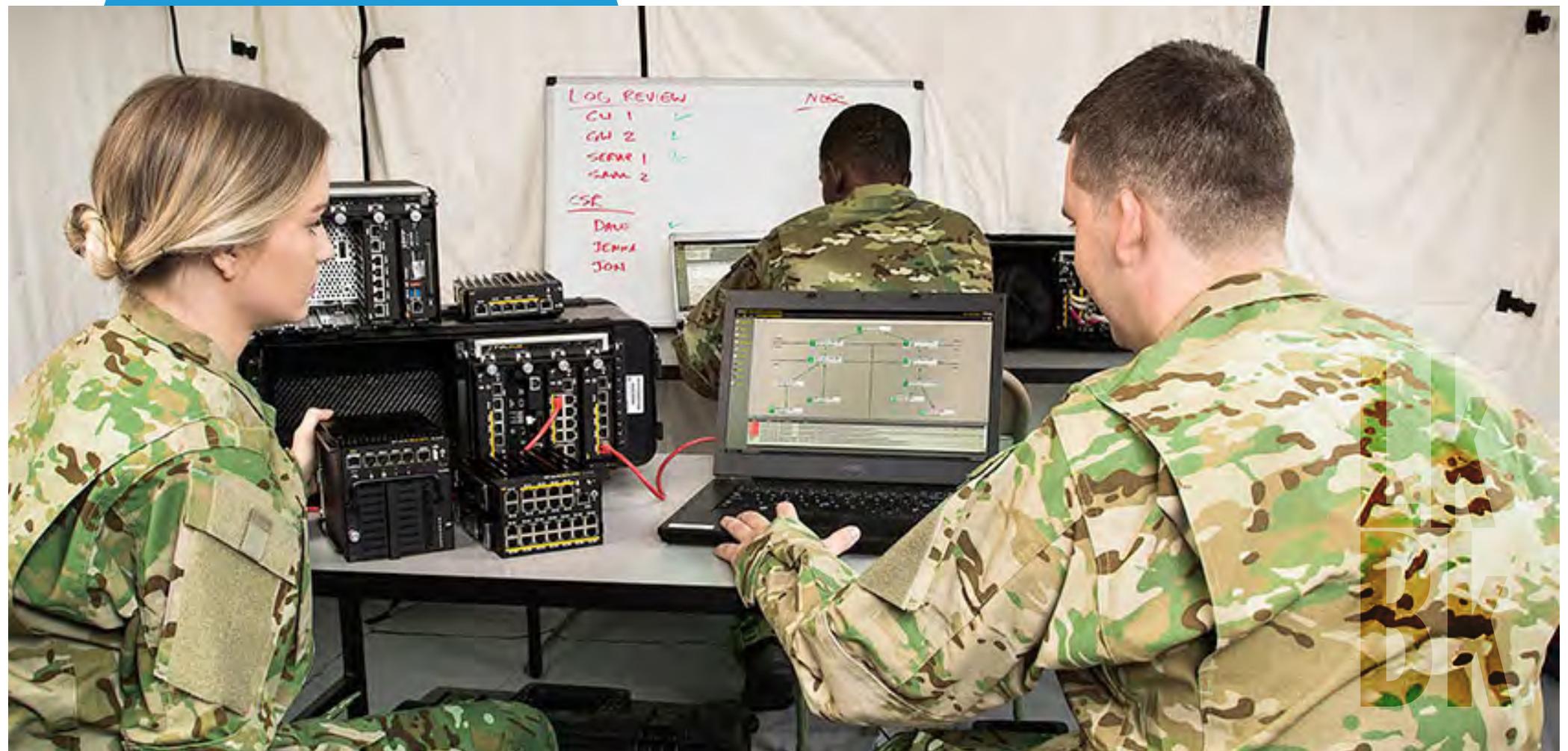
The JEDI Cloud is the only cloud that meets specific mission requirements in the cloud ecosystem. Specifically, it will provide a full range of commercial services at all three classification levels. The JEDI Cloud is just one component of DoD's Cloud Strategy to optimize use of cloud technology to the warfighter's advantage.

This service will provide Infrastructure as a Service and Platform as a Service,

which are the technologies needed for DoD to develop modern software. Infrastructure as a Service and Platform as a Service technologies are needed for DoD to develop modern software, keep pace with commercial innovation and make use of artificial intelligence and machine learning capabilities at scale. The services and capabilities supported by the JEDI Cloud will provide responsive, flexible, adaptive and timely solutions for participating organizations

to satisfy current and future cloud requirements.

The DoD Cloud Computing Program Office is responsible for the JEDI Cloud program and reports to the DoD Chief Information Officer. Under the DoD CIO's direction, the CCPO is constantly innovating to create a seamless general-purpose enterprise cloud accessible across multiple regions and all domains.



DC

LTC Nikolaus Ziegler USA

SENIOR INNOVATIONS OFFICER EMERGING TECHNOLOGIES DIRECTORATE



DESKTOP CONVERGENCE



Desktop Convergence is a new DISA program designed to transition the Department of Defense from a hardware-saturated computing environment to a single, multi-domain-enabled, mobile endpoint. It seeks to leverage virtual workspaces, cloud services and hardware attested credentialing solutions. This will reduce the number of devices required to operate and the costs to acquire and maintain them. A truly converged desktop experience transitions the user from desktops, laptops, tablets and smartphones to a single secure solution.

Desktop Convergence has evolved from several years of investment by DISA into efforts to assure a user's identity using advanced mobile capabilities. The Assured Identity Project sought to obtain and sustain confidence in a scalable process that assigned attributes to a digital identity associated to an individual or trusted device. By prototyping the hardware attestation to that digital identity using a mobile device, Desktop Convergence were able to implement continuous multi-factor authentication.

This amazing capability displays a desktop-like environment to a monitor using a docking station. Imagine moving from on-premise, device data to encrypted cloud storage; having the capability to leverage Public Key Infrastructure keys; and executing CMFA capabilities. That's what Desktop Convergence gives us.

CMFA is a cutting-edge, identity-based DISA capability that fuses together biometrics and contextual data collected at the endpoint to determine access into the DoD environment.

Desktop Convergence leverages CMFA to provide a single solution that will constantly verify the state of the endpoint and user identity. It enhances the warfighter's ability to securely access critical information on-the-move, supporting the "anywhere anytime" concept without the need to find a laptop or desktop at any globally disperse location.

DISA is currently working closely with mission partners to test the next generation hardware required to transition from today's desktop experience to a single device that is multi-functional and expeditionary, while also being ready to take on the challenges of the future.

Desktop Convergence is ready to roll out a number of exciting offerings across multiple domains and classifications; on encrypted networks and in cloud enabled environments.

DC



Andrew Malloy
TECHNICAL
DIRECTOR,
SERVICES
DEVELOPMENT
DIRECTORATE

D
S
O

DevSecOps

SUMMER |

LOOKBOOK |

For years the Department of Defense has struggled with the challenge of developing and fielding software intensive systems in a timely manner. Information systems acquisition processes mimicked those of major weapon systems, forcing a series of regulatory compliance, milestone decisions and documentation requirements that overburdened programs and drastically increased timelines. These issues are well known and have been discussed.

“Current processes are not responsive to need, the Department is over-optimized for exceptional performance at the expense of providing timely decisions, policies, and capabilities to the warfighter. Our response will be to prioritize speed of delivery, continuous adaptation, and frequent modular upgrades.”

-- 2018 National Defense Strategy.

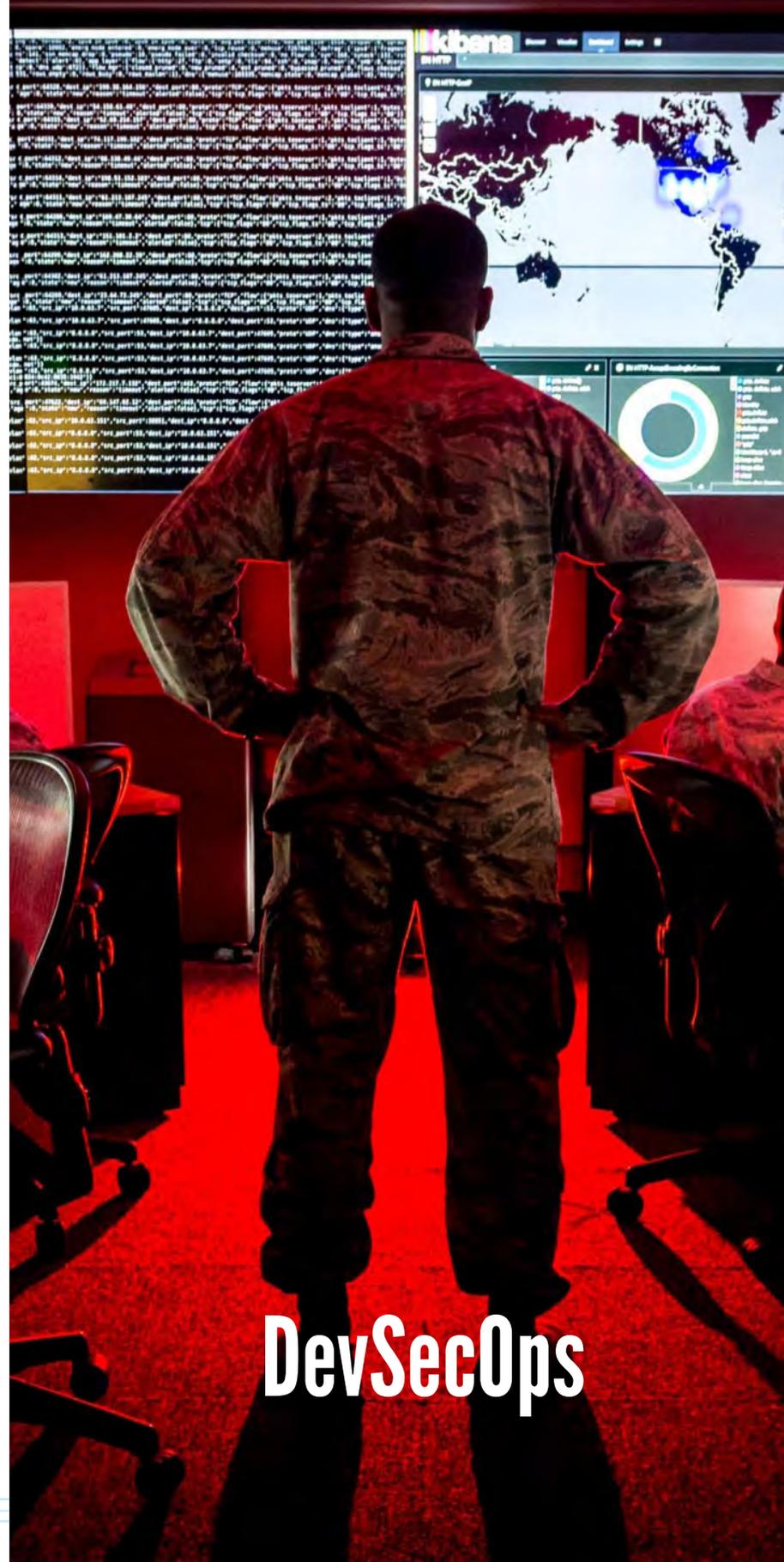
DSO

DevSecOps is an approach that integrates information-technology operations and security into the software development lifecycle to deliver capability to the customer in a more rapid fashion. The result is an environment that enables application development and accreditation at a speed and scale that keeps pace with defensive-cyberspace operations.

Many DevSecOps initiatives focus on software development tools, but DISA’s Enterprise DevSecOps Program will concentrate on providing the “Sec” and the “Ops” portions to the community of practice. For security, DISA will develop policy and guidance on the effective application of DevSecOps principles for the entire DoD.

The DISA Risk Management Executive office is the authoritative source for security requirements guides and DoD security technical implementation guides, which are used to ensure systems, applications and networks used in DoD are securely developed and locked down prior to their operational use. Today, Security Technical Implementation Guide development and the application of STIGs to systems is a tedious and highly manual process. The DevSecOps Program will create automated STIG procedures to apply at the beginning of the development process as well as automated scripts to test STIG compliance when development is complete.

On the operations side, DISA’s Enterprise DevSecOps Program will pilot



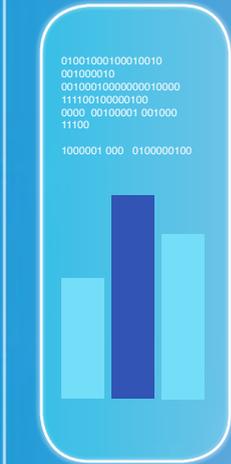
DevSecOps

software tools and techniques for cybersecurity service providers to continuously monitor applications at an enterprise scale. This will augment network and infrastructure data to give a more complete picture of the DCO environment. These tools, in addition to penetration testing and operational security scanning, will ensure accreditation is provided through a continuous authority to operate. Developers, accreditors and operators of DoD enterprise applications will benefit from the services provided by the DISA Enterprise DevSecOps Program. Software developers will be able to utilize pre-approved software bundles to build mission applications, and accreditors will be able to efficiently approve systems and mission applications being delivered to DoD. In operations, DoD system administrators will be able to effectively ensure systems are patched and in compliance with the latest DISA SRGs and STIGs for a more secure environment. Ultimately the operational user will be provided working, secure-mission applications at a greater speed than ever before as DISA responds to warfighter requirements at mission speed.

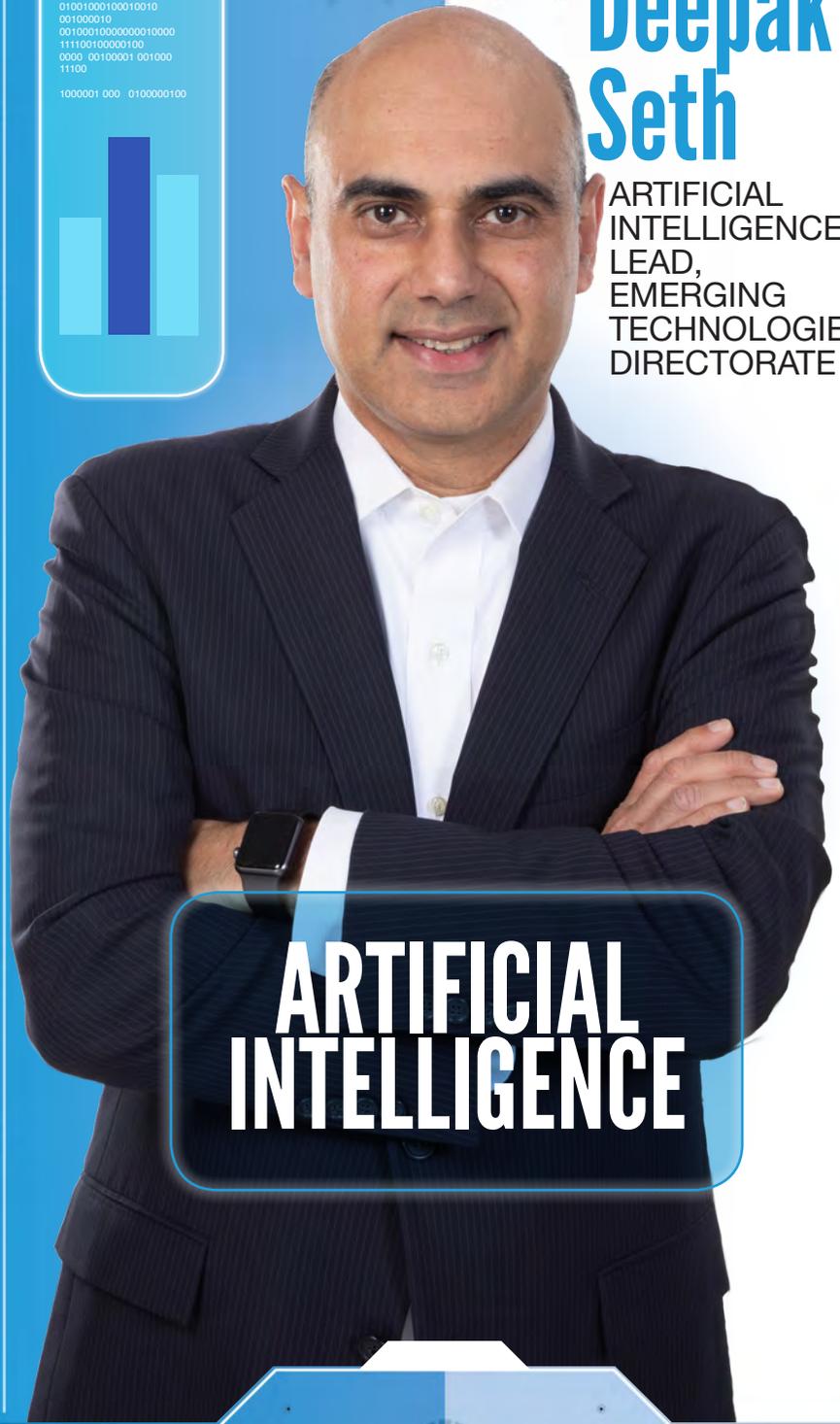
```

\\ RUN TIME : code no.233668
\\ UOD cross data summary : 100 001 100 000 111
\\ ESL : scan [ start 1356.location(x,y,z)]=point direstion

```



Deepak Seth
 ARTIFICIAL INTELLIGENCE LEAD, EMERGING TECHNOLOGIES DIRECTORATE



ARTIFICIAL INTELLIGENCE

AI

SUMMER |
 LOOKBOOK |

ARTIFICIAL INTELLIGENCE

DISA is applying artificial intelligence and machine learning technologies to a variety of cybersecurity challenges within the agency.

A prominent issue analysts face today is dealing with the huge volume of cyber sensor data riddled with false positives. AI massively scales our ability to process data, detect threats and discern malicious behavior at speeds and accuracy that exceed human capacity. AI technologies can quickly turn enormous volumes of cyber data into actionable intelligence and insights. DISA is leveraging AI/ML in its cybersecurity mission to automatically prioritize alerts so that events with a greater probability of malicious activity are identified by analysts in real-time.

This is one of the many reasons why DISA is working with the Joint Artificial Intelligence Center in developing the Joint Common Foundation. The JCF will be a powerful, cloud-based AI platform delivering standardized AI development tools and automated processes for all of DoD.

The JCF will have the authority to operate at all classification levels and is a key enabler of JAIC's ability to scale AI across the U.S. military. When fielded, the JCF will be a software factory that will accelerate the design, development, testing, fielding and sustainment of DoD-wide AI capabilities.

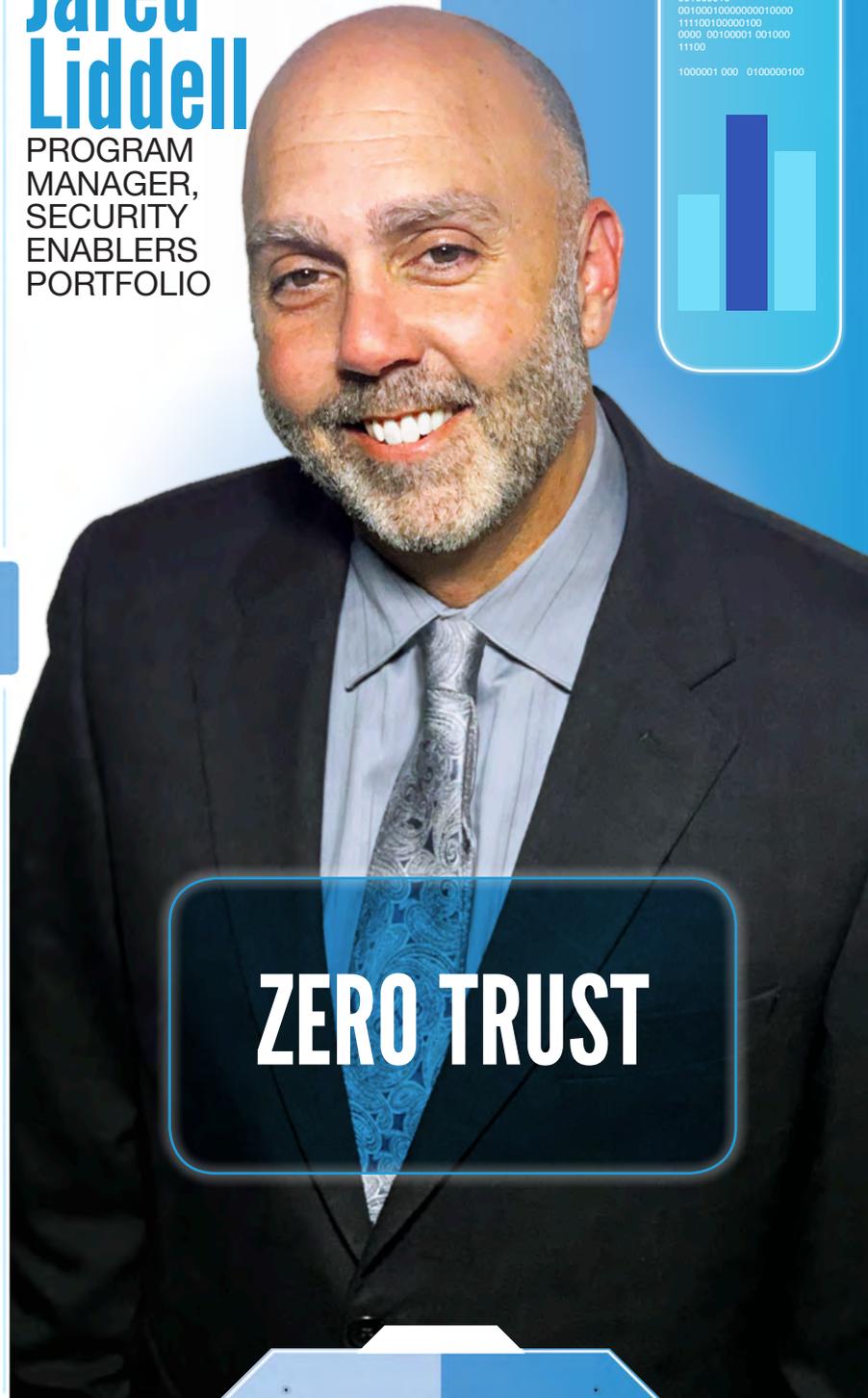
By developing AI applications in the JCF, DISA benefits from security controls and quality assurances that significantly reduce the time to deploy and field its own AI capabilities. Additionally, with investments in data governance and data platforms, DISA ensures the quality and availability of the data that fuels AI. DISA is actively working to leverage AI to revolutionize the way it counters cyber threats in order to win today and tomorrow.



AI

Jared Liddell

PROGRAM
MANAGER,
SECURITY
ENABLERS
PORTFOLIO



ZERO TRUST

The Department of Defense is evolving toward a new cybersecurity model called “zero trust.” DISA is working with U.S. Cyber Command and the National Security Agency, in support of the DoD chief information officer, to establish a DoD zero trust reference architecture that will provide guidance to DoD entities.

Zero trust aims to greatly reduce the DoD Information Network attack surface and to limit an adversary’s impact by making sure machines and their users are verified before granting access to DoD resources.

Zero trust incorporates the principles of “never trust, always verify,” “assume breach” and “verify explicitly.” These principles will be applied to many aspects of the DoDIN, starting with existing capabilities to strengthen today’s cybersecurity defense. Future Zero Trust capabilities will further raise cybersecurity defense while providing more efficient methods for operations and maintenance.

The zero trust enterprise reference architecture will illustrate how capabilities found within the seven zero trust pillars can be integrated while ensuring interoperability with other environments in the DoDIN.

The seven zero trust pillars are:

- User
- Devices
- Network/Environment
- Application/Workload
- Data
- Visibility and Analytics
- Automation and Orchestration

In practice, zero trust takes a data-centric approach to cybersecurity, moving traditional perimeter-based security protections closer to the data in order to more effectively protect data confidentiality, availability and integrity. The approach will modernize the DoDIN and improve cybersecurity practices and operations.

DISA is leveraging an agile methodology to approach zero trust from three different perspectives. First, the team is analyzing mission-partner environments to determine areas requiring improvement and providing recommendations. Second, the team will look at partnering with other program offices to use the functionality within technologies already implemented on the DoDIN in a manner consistent with a zero trust methodology. Lastly, the team is experimenting with options for a next-generation architecture.

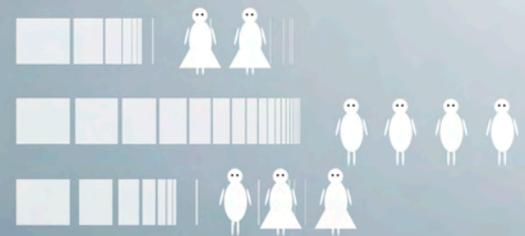
By looking at this issue from these three perspectives, the team aims for a more comprehensive solution that avoids traditional program and cybersecurity pitfalls. This will also enable the zero trust team to establish and cultivate relationships with mission partners that are imperative for the long-term success of the program and any future zero trust implementations.

ZT

SUMMER

LOOKBOOK

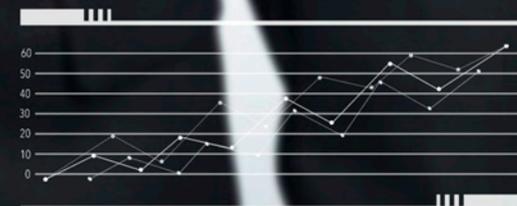
DISA JFHQ DODIN



Statistics



Analytics



DISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil
disa.mpeo@mail.mil

