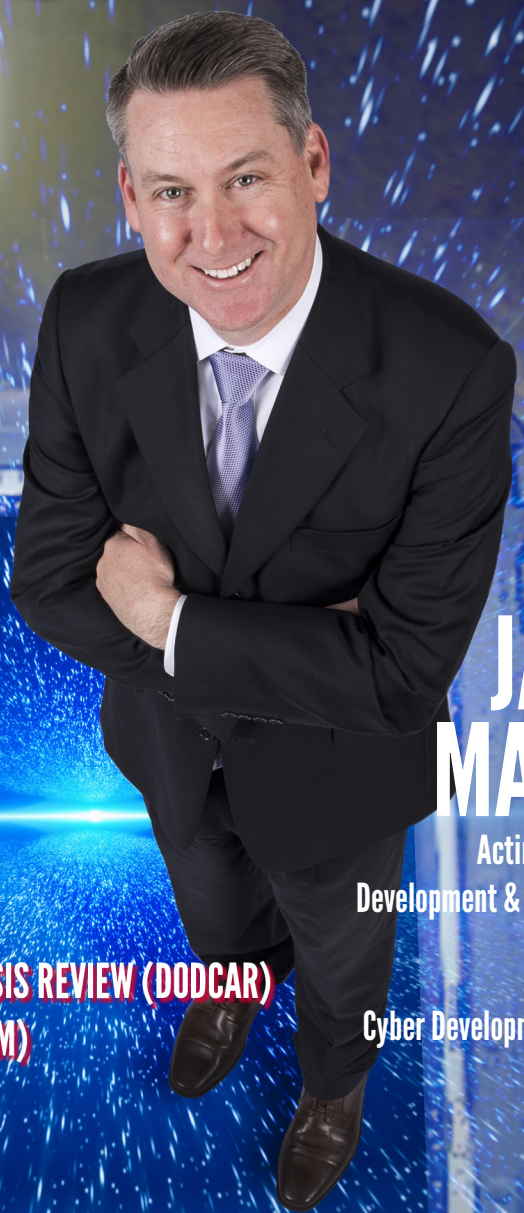
DISA
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Spring 2019

LOOK BOOK

LAYERED DEFENSE



JASON MARTIN

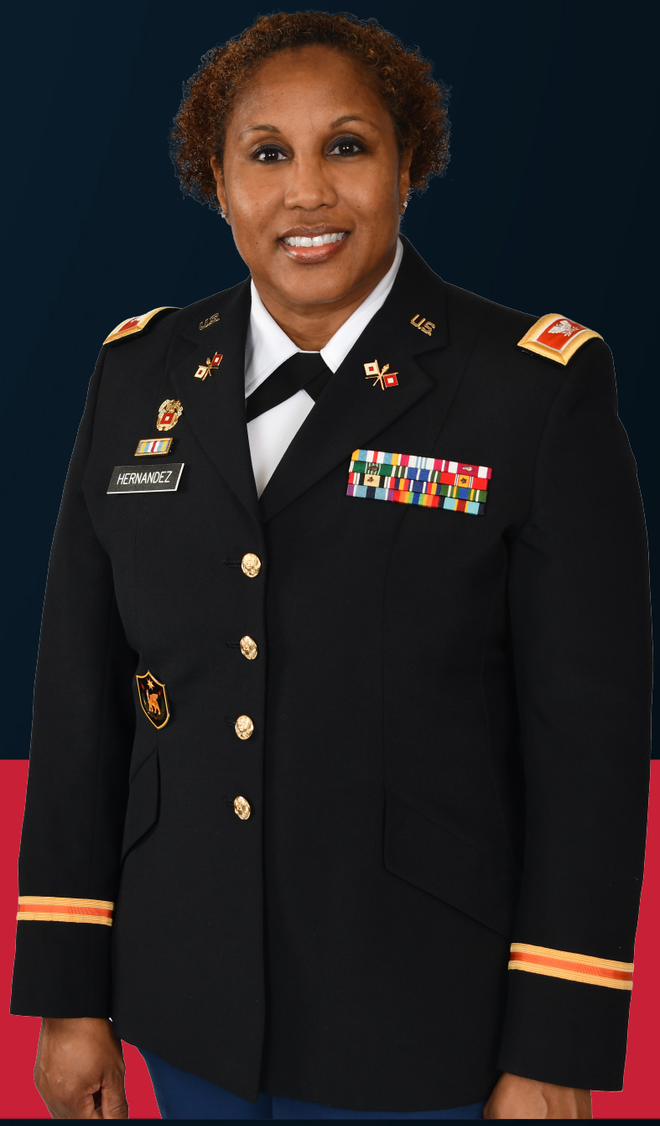
Acting Vice Director,
Development & Business Center
and
Acting Director,
Cyber Development Directorate

ACROPOLIS DEFENSIVE CYBER OPERATIONS
CLOUD BASED INTERNET ISOLATION (CBII)
DEPARTMENT OF DEFENSE CYBERSECURITY ANALYSIS REVIEW (DODCAR)
IDENTITY CREDENTIAL ACCESS MANAGEMENT (ICAM)
SOFTWARE DEFINED ENTERPRISE (SDE)
CYBER EXCHANGE (CYBERX)
ENDPOINT SECURITY
CYBER AWARENESS CHALLENGE
ENTERPRISE BREAK AND INSPECTION (EBI)
THE JOINT REGIONAL SECURITY STACKS (JRSS)

LAYERED DEFENSE

PROGRAM EXECUTIVE OFFICER CYBER OVERVIEW:

Army Colonel Delisa Hernandez is DISA's Program Executive Officer for Cyber responsible for overseeing acquisition and life cycle management activities of approximately 40 major cyber defense programs across 80 contracts totaling more than $750 million. PEO Cyber focuses on program, financial, and property management as well as procurement to include design, development, testing, and implementation activities.



Colonel Delisa Hernandez

UNITED STATES ARMY

PROGRAM EXECUTIVE OFFICER CYBER

"Across the Cyber Development portfolio we are working to ensure that affordable and relevant cyber defensive capabilities are delivered in a timely manner."

Raheem (Ray) McCormick

CYBER SECURITY INFRASTRUCTURE BRANCH CHIEF

ACROPOLIS DEFENSIVE CYBER OPERATIONS

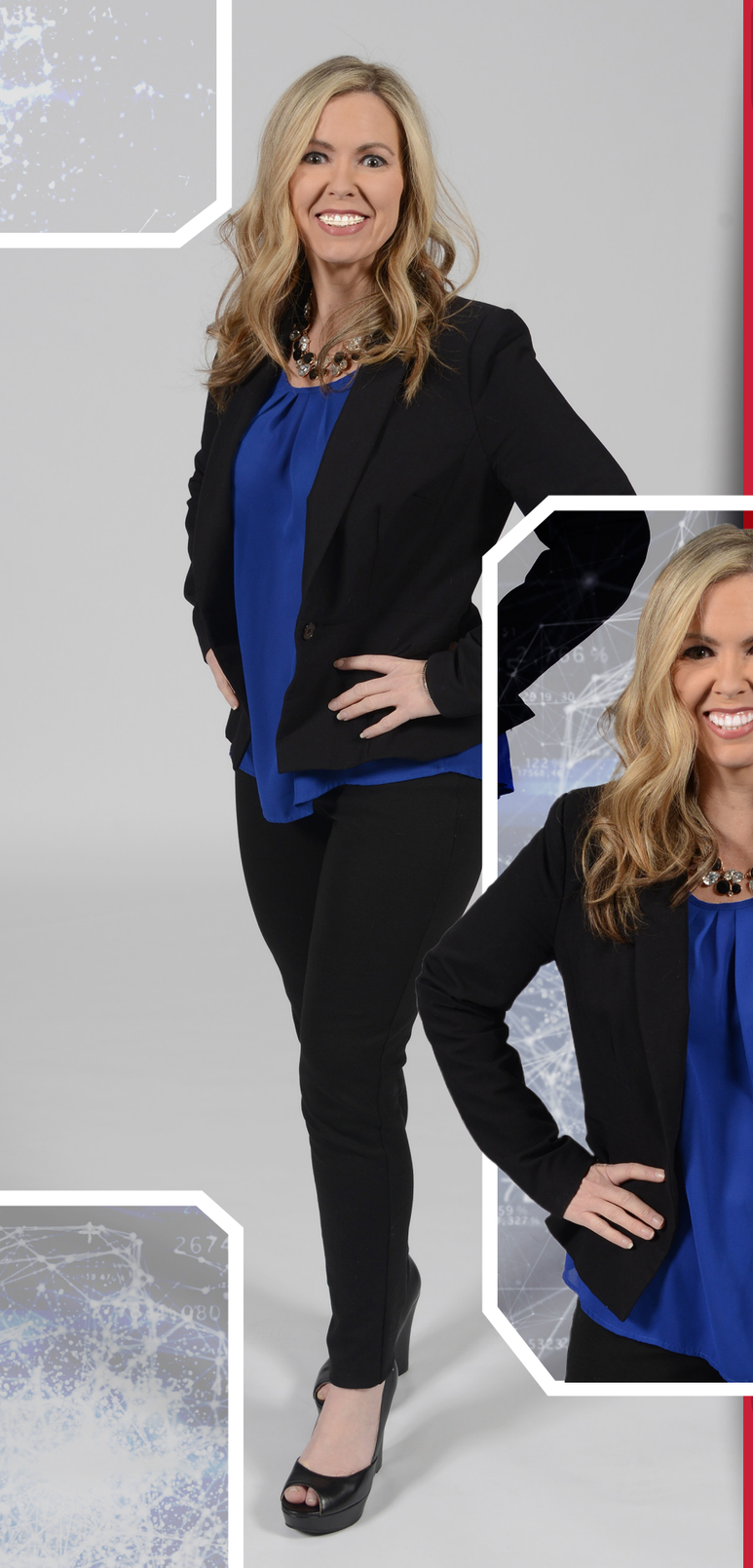
The Acropolis is currently an on-premise cloud (soon to be hybrid cloud) that provides a secure, consolidated and integrated Defensive Cyber Operations (DCO) and global Situational Awareness (SA) environment for analysts within the Department of Defense to protect and defend the DOD Joint Information Environment (JIE), DOD Enterprise Services and the Department of Defense Information Network (DODIN). It is DISA's DCO environment and it is "where we fight" for DCO operations.

DISA's enterprise environment is currently hosting various cyber security tools that enable analysts to conduct operations on the DoDIN.

The current team that runs Acropolis consistently pushes the innovation boundaries and are often asked to provide solutions that obtain, transform, and deliver various types of data into various DCO tools including the Big Data Platform. Additionally, we survey the market for solutions to enhance an analyst's ability to identify threats, and protect the DoDIN.

Several mission partner applications have a cloud migration strategy. By delivering cloud capabilities, we will be able to ensure that their applications hosted within the Acropolis environment meet required security compliance and are ready to meet their hosting needs.

DISA is looking to modernize the Acropolis environment with our "where we fight" initiative, which will enhance accessibility, security, and streamline analyst workflow. Additionally, we are looking to leverage commercial cloud offerings to enable compute scalability and new cloud services that support applications in machine learning, and decrease infrastructure cost.



Dr. Angela Landress

CYBER INNOVATION PROGRAM MANAGER

CLOUD BASED INTERNET ISOLATION

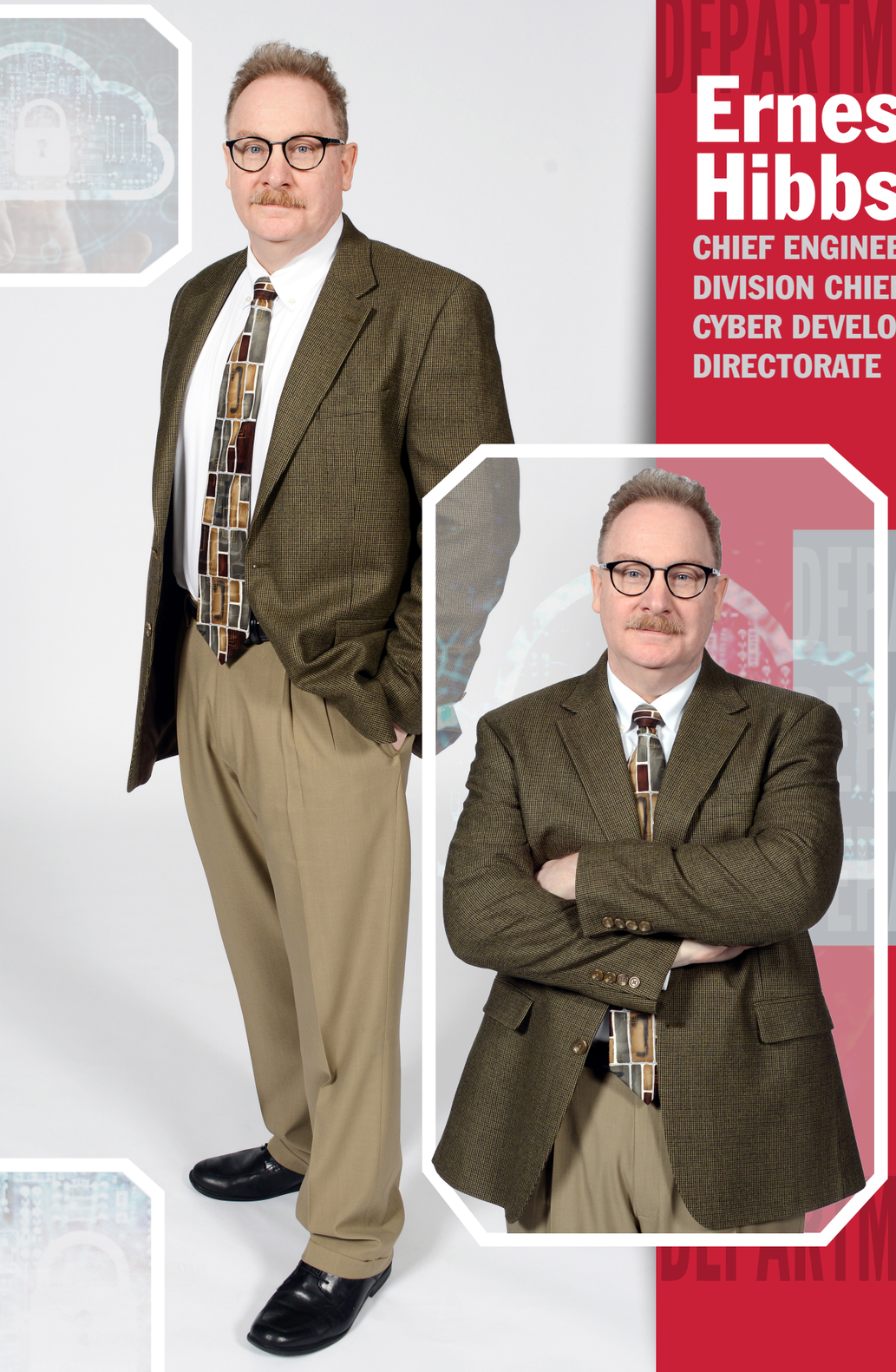
Cloud Based Internet Isolation, known as CBII this is a new program that will move unclassified browsing traffic into a secure cloud environment.

This program will help Defense Information Systems Agency (DISA) save significant amounts of bandwidth at the internet access points (IAPs) and reduce the cost of expensive cyber defensive tools for the Department of Defense (DOD) by reducing the amount of traffic those tools need to inspect. Additionally, by isolating web browsing, no potentially malicious code will be executed on the user's computer, improving the overall security posture of the department.

This program is very innovative because it is the first time DISA or any component of the Department of Defense has used a secure browser isolation tool at an enterprise scale.

Mission partners will experience faster internet browsing and improve the security posture on their endpoints significantly.

Moving forward, the CBII program will implement isolated web browsing in conjunction with nine mission partners across the DOD. The program first users transitioned to this capability in April 2019.



Ernest Hibbs

CHIEF ENGINEER, DIVISION CHIEF, CYBER DEVELOPMENT DIRECTORATE

DEPARTMENT OF DEFENSE CYBERSECURITY ANALYSIS REVIEW

LOOK BOOK
LAYERED DEFENSE

The Department of Defense Cybersecurity Analysis Review (DoDCAR) is a method of determining how well a system is prepared to match up against cyber threat activities. All known and recent threat activities are defined and maintained by the National Security Agency in a framework called the National Security Agency/Central Security Service (NSA/CSS) Technical Cyber Threat Framework (NCTCF). The NCTCF maps adversary actions to points in the cyber kill-chain, describing ways to get in an architecture, stay in an architecture and act from within an architecture.

The DoDCAR use of a threat framework is backed by historical intelligence which is literally a library of adversarial actions that a chief engineer or program manager can use to build their system's unique, efficient cyber defense requirements. In our operational security (OPSEC) mindset, it is equivalent to getting specific intelligence briefings for a unique overseas environment. Know your environment; know your threats.

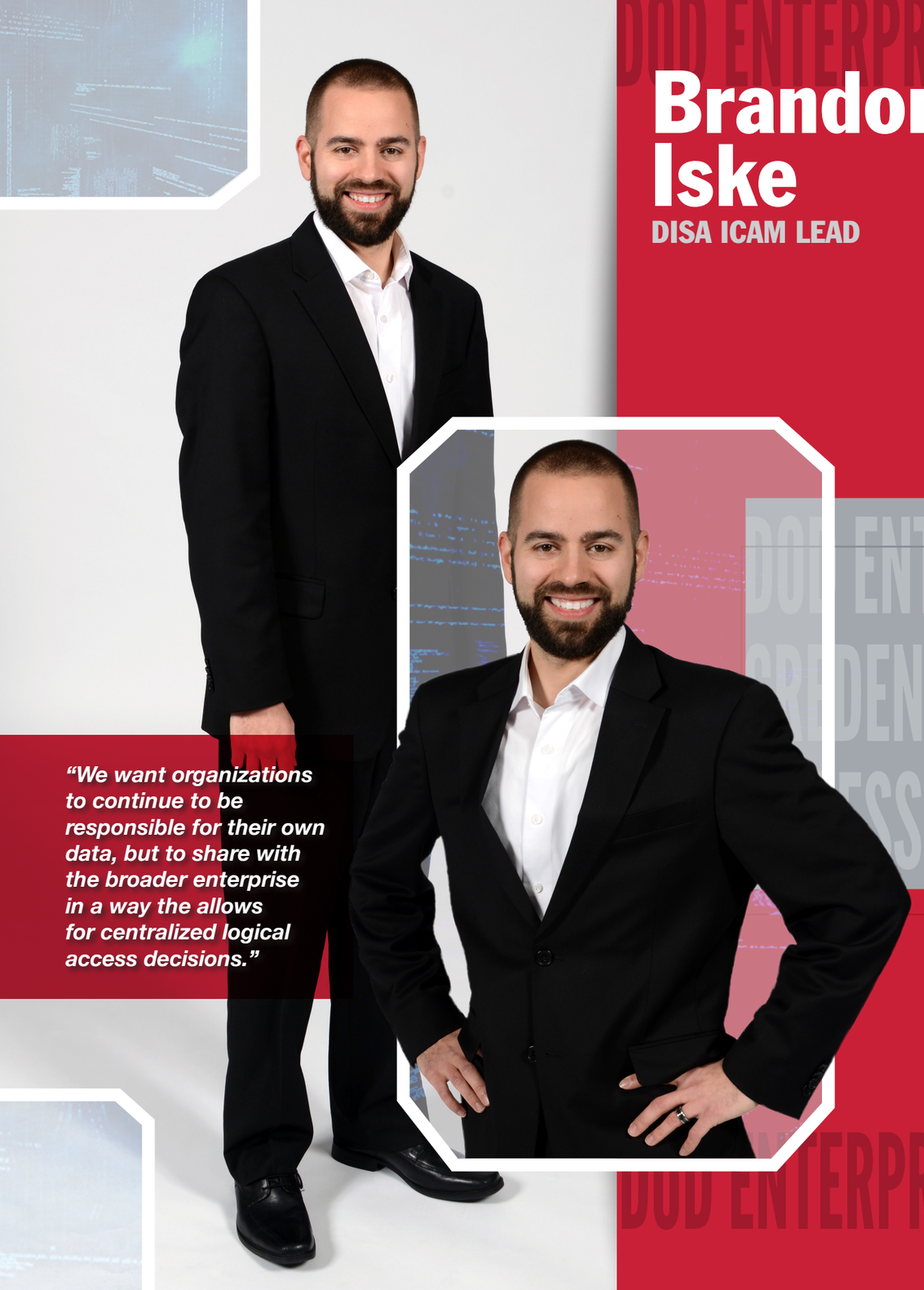
DoDCAR is innovative in that it introduces an engineering discipline and unified approach in a world of highly reactive cyber technical solutions. It enables us to proactively protect our environment based on a broader awareness and understanding of the threats. Furthermore, with the added intelligence from historical threat activities tied to a framework we have an actual terrain definition of our challenges and are able to select only the highest performing capabilities.

The goal of these pre-staged defenses is to improve operational availability in an environment amidst aggressive attempts at system corruption and mission failure. In addition, complex weapons systems with multiple interfaces now rely on DoDCAR assessments.

Within DISA and the DoDIN the goal is to have all cyber engineering plans and cyber operations using the DoDCAR framework to efficiently address our cyber threats. DoDCAR will also be a key evaluating factor for the future capabilities of Joint Regional Security Stack (JRSS).

Brandon Iske

DISA ICAM LEAD



"We want organizations to continue to be responsible for their own data, but to share with the broader enterprise in a way the allows for centralized logical access decisions."

DOD ENTERPRISE IDENTITY CREDENTIAL ACCESS MANAGEMENT

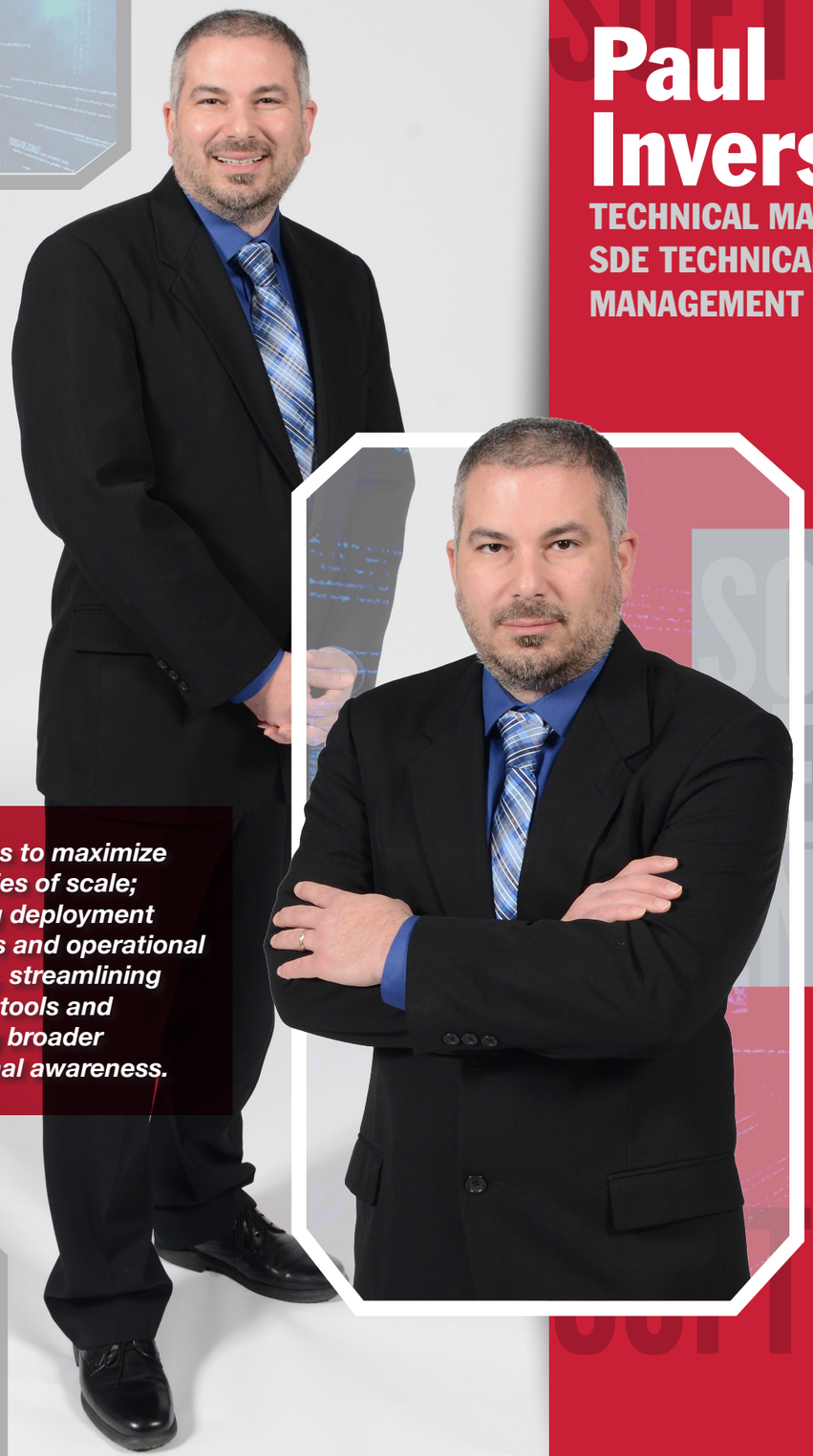
The Department of Defense Enterprise Identity Credential Access Management (ICAM) program aims to leverage advances in commercial technology to synchronize a single master user record across the Department of Defense (DOD) enterprise to automatically create, delete and manage accounts. ICAM is a DOD Chief Information Officer (CIO), National Security Agency (NSA), Defense Manpower Data Center (DMDC) and Defense Information Systems Agency (DISA) effort to enhance enterprise capabilities. ICAM will provide a secure, federated authentication service for the DOD, simplifying complexity and increasing user traceability.

Today's user authentication is performed by each application, using a centrally issued user common access card (CAC). Integration with an identity provider for authentication must be engineered into each application. ICAM creates a centralized, authoritative source to provide user authentication across the DOD. It will establish a foundation for strengthening our cyber defense and compliance by providing a unified source for auditing purposes. ICAM has been identified as a DOD Cyber top10 initiative by the DOD CIO, and is aligned at the federal level with the Department of Homeland Security (DHS) effort, the Continuous Diagnostics and Mitigations (CDM) program, which is a key area of focus in fortifying cybersecurity for government networks and systems.

After decades of success in managing identity through the CAC and public key infrastructure (PKI), ICAM will leverage commercial partnerships and mature capabilities to lay the foundation for a more assured access management infrastructure for the future. ICAM will decrease time to implementation and costs for new applications, expedite cloud adoption and offer alternative form factors for authentication that support diverse populations with varying requirements.

Through using ICAM, DISA will be able to provide enterprise capabilities to manage account and authentication services and lower the burden and cost of DOD programs and applications. Furthermore, the ability to centrally audit "who has access to what" reduces mission partner risk as well as department risk.

SOFTWARE DEFINED ENTERPRISE



Paul Inverso

TECHNICAL MANAGER, SDE TECHNICAL MANAGEMENT OFFICE

SDE aims to maximize economies of scale; reducing deployment timelines and operational budgets, streamlining security tools and enabling broader situational awareness.

Software Defined Enterprise (SDE) is a new paradigm, which enables automation and virtualization to complex environments to provide faster services with less mistakes and rework. SDE is the next generation approach to streamline operation, management and sustainment on the DODIN.

The unique capabilities will ultimately unify disparate services and business systems across DISA, spanning transport, secure gateways and cyber tools through policy-driven actions. SDE achieves this objective by moving networking logic to a location where it is centrally managed and sustained.

SDE efforts will work in concert with a number of key agency initiatives, including zero trust architecture, machine learning and cloud hosting and security. Foundational elements of SDE are automation and virtualization. Automating the provisioning, monitoring and remediation of repeatable processes and procedures will streamline operations and serve as a use case for future automation integrations.

The two primary advantages of SDE are speed and accuracy. Mission partners will be able to access new services much faster due to SDE, and the minimization of routine human interactions will reduce the possibilities of mistakes and misconfigurations.

In 2019, DISA will release a Request for Information and a Request for Proposals for the SDE Global Orchestrator (SDE-GO) that will connect to the DISA Storefront, all of the service level orchestrators, and cyber tools. Although, SDE capabilities will appear transparent to our mission partners, it will provide the agility for the DODIN and over time reduce sustainment costs.

Laurel Lashley

PROGRAM MANAGER

DOD CYBER EXCHANGE

The DOD Cyber Exchange, formerly known as the Information Assurance Support Environment (IASE), provides one stop access to cyber information, policy, guidance and training for DOD and the general public. Cyber Exchange is a complete redesign and rebranding of the IASE, which has supported the information assurance and cyber community for more than 20 years. DISA was appointed to establish and facilitate Cyber Exchange by the DOD Chief Information Officer, and manages the portals in three environments:

1. Cyber Exchange Public – accessible to all internet users;
2. Cyber Exchange NIPR – requires public key infrastructure (PKI) credentials for access to “For Official Use Only” content;
3. Cyber Exchange SIPR– requires a Secret Internet Protocol Router Network (SIPRNet) token for access to the domain and content; also available to appropriately credentialed foreign partners.

Cyber Exchange is the DOD’s knowledge repository for cyber guidance and training; no other centralized and comprehensive resource exists in the Department of Defense. Cyber Exchange content is driven by the demands and requirements of the DOD community to develop and share cyber expertise and training across the enterprise. It leverages the latest web technology to provide cyber subject matter experts with a platform to deliver their content.

Cyber Exchange was developed with mobile and HTML5 compatibility, provides dynamic and adaptive content management and delivery, search engine optimization and a host of new topic areas.

DOD Cyber Exchange users can expect more features and functionality in the coming years. Plans are underway to further improve how Cyber Exchange delivers content and persistent training to users. Cyber Exchange will integrate a learning management system and virtual training environment to the NIPRNet environment. The learning management system will provide a course catalogue and automate course registration, metrics and analytics capabilities. The virtual training environment will deliver scenario based exercises, labs and remote access to students’ desktops.

Fredrick Cook

**CHIEF,
ENDPOINT SECURITY
BRANCH**

ENDPOINT SECURITY

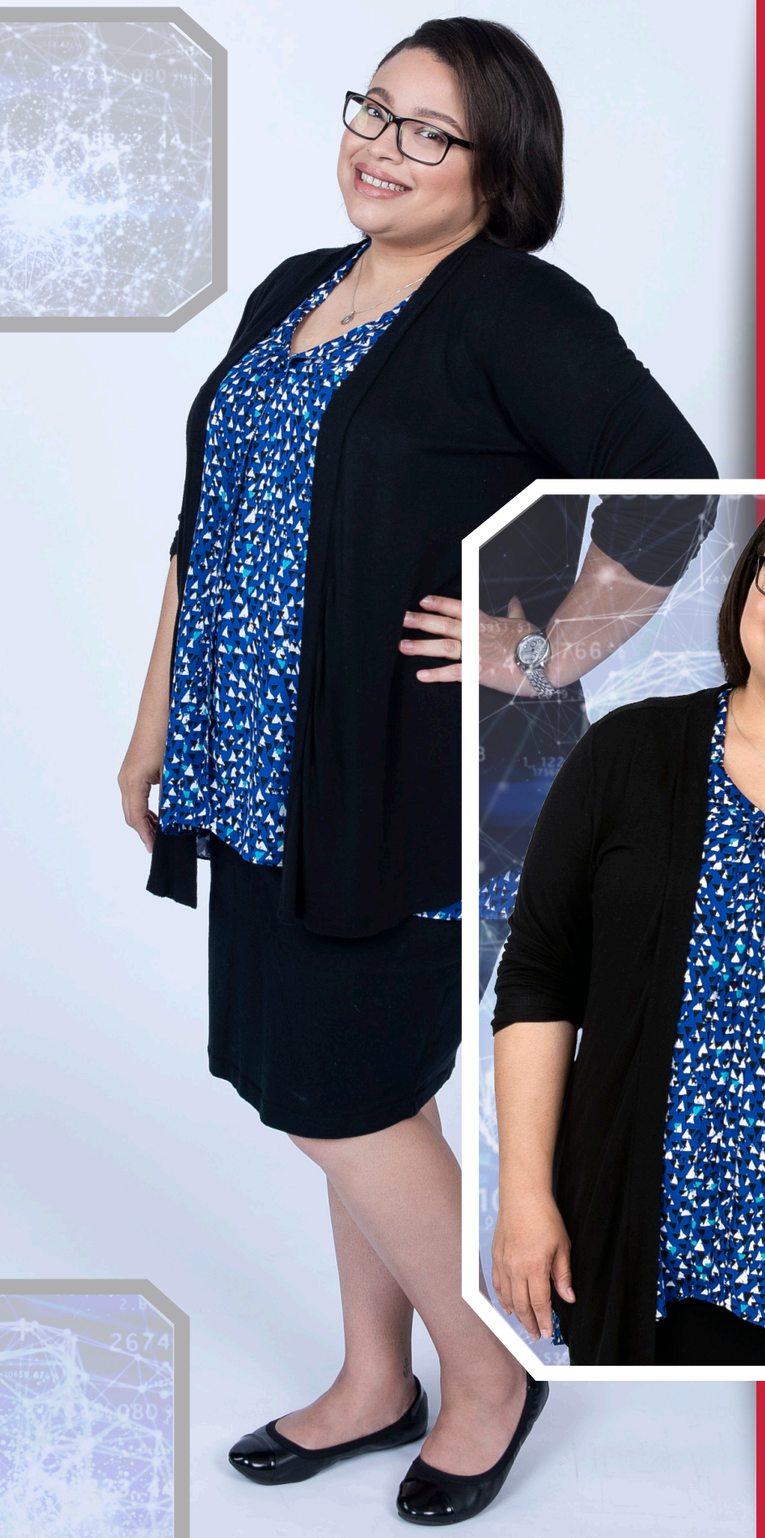
Endpoint Security is the tools and techniques used to secure the various Department of Defense Information Network (DODIN) connected devices. Traditionally, Endpoint Security encompassed workstations and servers but now, with the advent of the Internet of Things (IoT), it includes other (DODIN) connected assets such as Voice over IP (VoIP) phones and mobile devices, where department data is stored.

Adversaries will employ tactics to evade perimeter defenses. Endpoint security is the last line of defense to keep the adversary from stealing, exfiltrating, manipulating or destroying our sensitive and classified data.

The Endpoint Security program will innovate to keep up with the ever evolving cyber threat landscape. We explore and deploy the latest technologies using machine learning and artificial intelligence to detect and eject attacks that would have previously gone undetected.

The Endpoint Security program is the program office for Host-Based Security System (HBSS) and assists mission partners in finding and deploying the next solutions beyond HBSS. DISA works with endpoint communities to find the right solutions to secure mission partner data whether it resides in a data center with unlimited network resources, or in the field.

As the HBSS program ends, the Endpoint Security team has moved our focus to the next security solutions. Having already assessed containment and Endpoint Detect and Respond (EDR) solutions for the department, the latest anti-malware, telemetry, threat sharing and user activity monitoring solutions will be assessed for use by the DODIN mission partners.



Chennel Stroud

PROGRAM MANAGER, E-LEARNING TRAINING BRANCH

CYBER AWARENESS CHALLENGE

Cyber Awareness Challenge is an awareness course developed by DISA as directed by Department of Defense Chief Information Officer (DOD CIO). This course is taken annually by over 5 million DOD users as their annual cyber awareness training. The course informs users on how to keep the DOD network secure. The Cyber Awareness Challenge is also open for public use on Cyber Exchange (CyberX) formerly known as the Information Assurance Support Environment (IASE).

In 2019 the DISA cybersecurity team completely redesigned the Cyber Awareness Challenge course. The new course is a post-apocalyptic theme where someone comes from the future to inform the user that security breaches we are currently experiencing is causing problems in the future. The course walks users through how to secure those threats.

The Cyber Awareness Challenge course is important because it provides the training baseline for all user in the DOD including military, civilian and contractors. All new DOD employees must take this course in order to access the DOD network.

Cyber Awareness Challenge 2019 is innovative and offers the following new features to users:

- Knowledge Check Option: Also known as the “test out option” giving the return user the opportunity show their proficiency in all the cyber awareness modules. If proficiency is shown the user is allowed to skip that module.
- Group Facilitator Guide: Guides a facilitator through administering the course to a group in conjunction with the Cyber Based Training (CBT).
- Group Facilitator Briefing: Is a PowerPoint briefing used to deliver the course to a group of users.
- Mobile Compatibility: Couse available on iOS and Android tablets providing convenience to millions of users.

The newly implemented features offers several benefits to mission partners. The knowledge check option for return uses saves time as it can cut the course by more than half the time.The two new group training options meets the DOD’s goal of offering the Commanders the option to teach their troops in person, getting away from computer based training only. The course being mobile compatible offers full flexibility to the user by providing them the opportunity for them to take the course anywhere at any time.

The DOD Cyber Workforce Advisory Group held its annual requirements gathering meeting and determined to add the new CPCON levels as delivered by United States Cyber Command (USCYBERCOM) for the Cyber Awareness Challenge 2020 release.

Davon Tyler AND Sandra Felton

INTERNET PROTECTION BRANCH

ENTERPRISE BREAK AND INSPECTION

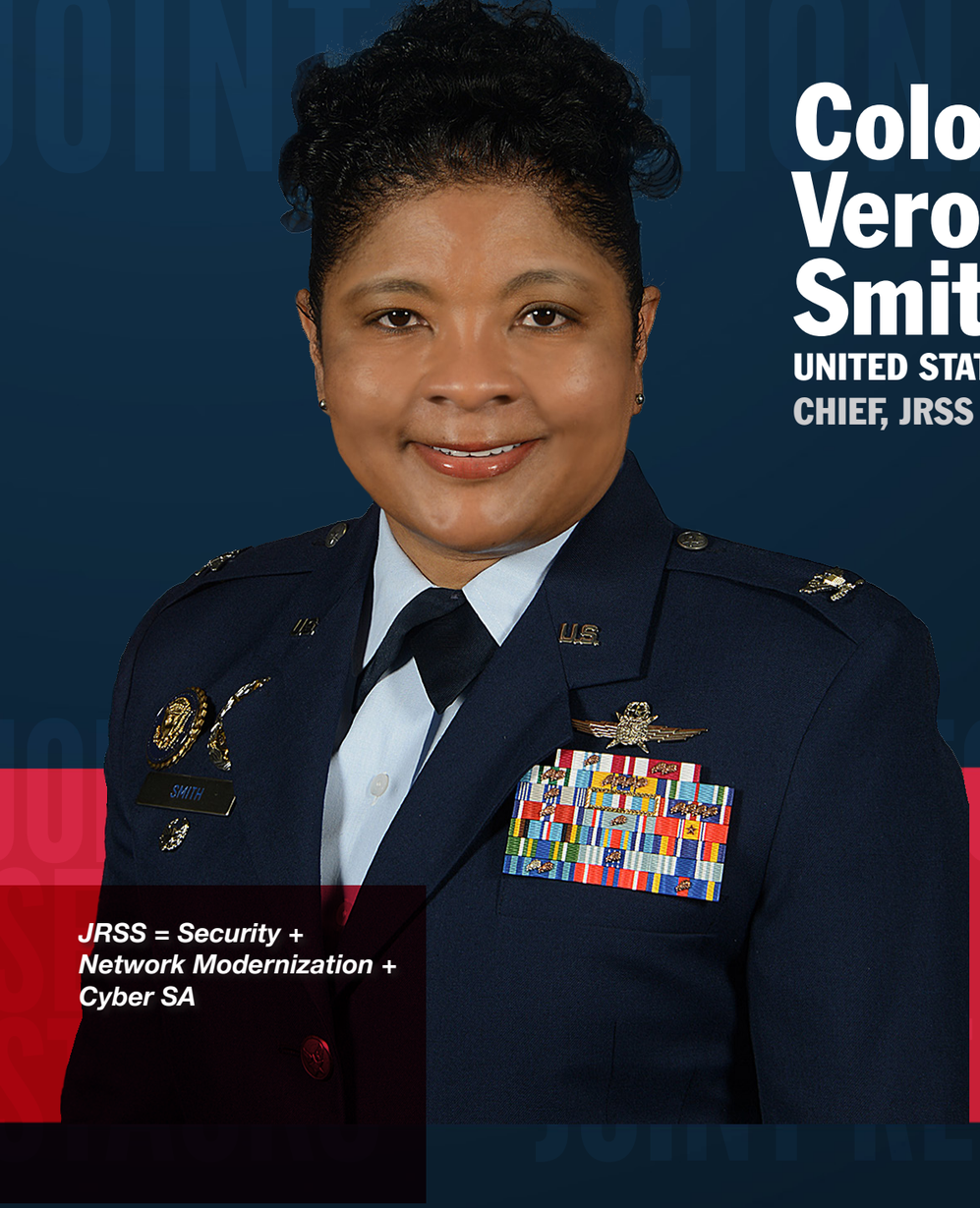
Enterprise Break and Inspection (EBI) is a complementary capability employed at DISA Internet Access Points (IAPs) that allows the existing cybersecurity systems to inspect encrypted traffic traversing DISA'S IAP. This allows the cybersecurity system to see, interpret, and take action on traffic comprising approximately 80 percent of web traffic from the Internet.

The Internet is an important resource for DOD missions. EBI solves a critical problem for cybersecurity systems by expanding utility. Without EBI, cybersecurity systems could only inspect approximately 20 percent of web traffic for malware, and other threats, but EBI can inspect all traffic at the IAPs, allowing users to safely use the Internet without introducing mal-ware and threats into the DOD network environment.

EBI is the first implementation of its kind at this scale within the DOD. It is innovative in its approach to tackle challenges that most organizations had come to accept. For the question: how do you inspect secure traffic while maintaining the integrity of the data? The EBI program worked with National Security Agency (NSA) to come up with a secure solution to inspect traffic while maintaining the integrity of the data as it traverses the DoDIN.

EBI is leveraged by multiple cybersecurity systems that reside at the IAPs. This design eliminates the need for each cybersecurity system to develop its own break and inspect solution, thereby saving millions of taxpayer dollars.

The Joint Force Headquarters Department of Defense Information Network (JFHQ-DODIN) has issued a task order requiring all of DOD components to migrate behind EBI for IAP traffic. To assist in this effort, DISA global migrates the customer network subnets to the EBI suit.



Colonel Veronica Smith

UNITED STATES AIR FORCE

CHIEF, JRSS DIVISION

JRSS = Security + Network Modernization + Cyber SA

JRSS DIVISION

Security: The Joint Regional Security Stacks (JRSS) is a joint cyber war fighting platform consisting of network security capabilities that provides enhanced network command and control which allows Department of Defense (DOD) to continuously monitor and evaluate data routed through the Department of Defense Information Network (DODIN).

Network Modernization: JRSS provides this capability through standardized, regionally focused, physical infrastructure known as “stacks” that allow DOD to intake and rapidly transport large sets of data.

Cyber Situational Awareness: The JRSS management tools enable network defenders and defensive cyber operators to see, manage and assess data passing through the stacks to maintain situational awareness of systems and ensure response time and manage data quantity and performance standards.

JRSS is now centralizing the department’s network security into regional architectures, instead of locally distributed architectures at each military base, post, camp, or station to deliver a more secure, defendable and responsive Department of Defense integrated network, providing enhanced command and control capability. Essentially, JRSS reduces the cyber-attack surface and reduces cost for implementing and sustaining this capability for the entire DOD.

JRSS reduces the number of enemy attack vectors to the DODIN by consolidating multiple security gateways into single access points to the DODIN. Reducing the number of security gateways provides fewer opportunities for a hacker to access the DODIN.
JRSS is redundant and incorporates multiple layers of seamless failover which creates a secure environment that significantly reduces the risk of total system failure.

The stacks are centrally configured and managed which mitigates risk by eliminating the vast diversity of equipment that makes up the cyber domain. This configuration make the DODIN more vulnerable to a zero day attack. However, that risk is counter balanced by the speed with which a mitigation can be put in place and the consistency of management that the Joint Management Network (JMN) affords the administrators. Successful attacks rely on well-known and published vulnerabilities and the best defense against attacks is to identify and eliminate attack vectors as quickly as possible. This architecture allows DOD to do that at the enterprise level for the first time.

All DOD traffic seamlessly moving along well defended, flexible enterprise networks. Network operators and maintainers have the right information presented in a meaningful way to act proactively, anticipating conditions that lead to outages and resolving them before they impact service to the user. Network defenders have the right information presented in a meaningful way to proactively adjust defenses to protect against the newest threat vectors and be able to detect adversaries already in the network and stopping them from disrupting our communications.

www.disa.mil