Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper

Volume 4, Issue 1

IN THIS ISSUE

ASK THE LEADERSHIP
JEANETTE M. DUNCAN

DCSA RENAMES EXCELLENCE IN COUNTERINTELLIGENCE AWARD

COMMUNITY HONORS UNCLE OF DCSA EMPLOYEE

IN THIS ISSUE

Vol 4 | ISSUE 1

DCSA Gatekeeper

Published by the Defense Counterintelligence and Security Agency (DCSA) Office of Communications and Congressional Affairs (OCCA)

DCSA LEADERSHIP

Daniel J. Lecce
Acting Director

Juli MacDonald
Chief, OCCA

Cindy McGovern
Managing Editor

Elizabeth Alber
Editor

John J. Joyce
Staff Writer

Christopher P. Gillis
Digital Content Specialist

Tony Trigg
Layout, Editing and Design

This Department of Defense (DOD) magazine is an authorized publication for members of DOD. Contents of the Gatekeeper Magazine are not necessarily the official views of, or endorsed by, the U.S government, DOD, or DCSA. The editorial content of this publication is the responsibility of OCCA.

All pictures are DOD photos, unless otherwise identified.

FROM THE ACTING DIRECTOR

Happy New Year! This is my first column as Acting Director and I'm pleased to have this platform to highlight the great work DCSA employees are doing to support our nation's security. Since arriving at DCSA as the Deputy Director, I have made the development of our Agency culture, employee engagement, and advancement of our values top priorities.

Our focused work on DCSA's Strategic Plan 2022 – 2027 has had a positive impact across our four mission areas (Personnel Security, Industrial Security, Counterintelligence and Insider Threat, and Security Training), while the work of our Field Directorate has gone a long way to better integrate our Agency, improve communications, and push support into our field offices. We will continue to build a workforce culture that reflects our values – most importantly our investment in people and commitment to our mission and values.

You can see our values reflected in the articles contained in this issue of the GATEKEEPER. Our new Chief Information Officer has found ways to collaborate with service providers to solve complex IT challenges and deliver better and more reliable network service to our dispersed workforce.

Our new field structure is providing direct support (IT, logistics, human resource) to our field workforce freeing them to focus exclusively on the mission. We are moving aggressively and deliberately to continue the integration in the field by implementing knowledge management tools to allow for information sharing and collaboration.

Our National Background Investigation Services (NBIS) team continues to leverage all opportunities to engage with stakeholders with the goal of delivering the best possible product. The same is true for Industrial Security's work on the National Industrial Security System, modernizing the system and ensure inoperability across industry and DCSA mission areas.

Finally, the rich history our workforce's unwavering commitment to service to our great nation is on display in Jessica Thompson feature on Chad Plesakov's uncle. Chad works as a NBIS policy analyst and has been with the DCSA for over 20 years. He was inspired to service by his uncle who was killed in action in Vietnam in 1967. Chad's uncle was 19 years old when he was killed.

I am impressed everyday by the grit, determination, and hard work of our Gatekeepers. Thank you for making a positive difference every day. Our nation's security depends on it.

DJ Lecce

Daniel J. Lecce
Acting Director,
Defense Counterintelligence and Security Agency

ASK THE LEADERSHIP Q A

Editor's Note: In each issue of the Gatekeeper, we feature an interview with a senior leader on their background, mission and program priorities.

Ms. Jeanette M. Duncan serves as the Chief Information Officer (CIO).

In this capacity, she is the technical expert and principal advisor to the DCSA senior staff on all aspects within the agency enterprise information technology (IT) portfolio. She provides strategic IT expertise, advice and guidance on design, development, integration, implementation and sustainment of enterprise architecture, cybersecurity, infrastructure platforms, tools, governance, programs, and services to meet current and future technology needs. She manages the cybersecurity certification program and serves as DCSA's Primary Authorizing Official for accreditation of all DCSA information systems.

Prior to her current position, Ms. Duncan was the CIO for Department of the Air Force, Office of the Assistant Secretary for Financial Management and Comptroller, Washington, D.C. She provided executive leadership and direction, broad technical knowledge, skill and experience on all technology, innovation, and financial transformation matters. Ms. Duncan also promoted the development and implementation of identity, credentialing, and access management; robotics process automation; set standards for integrated enterprise-wide information technology projects; and advocated for resources required to support innovation and transformation of financial management systems across the Air Force and in support of the Defense Enterprise Account Management system to support the warfighter. Ms. Duncan led the Department of the Air Force (DAF) in closing IT audit findings that facilitated the DAF receiving a modified audit opinion for the first time in its history in FY23.

Ms. Duncan served as the CIO, National Endowment of the Arts; CIO, Headquarters Department of the Army, Office of the Assistant Chief of Staff for Installation Management; and served in the U.S. Army. She earned a Bachelor of Science in Public Administration and a Master of Arts in Business Leadership with a double major in Human Resources Management and Total Quality Management, Upper Iowa University, and a Master of Science in National Resource Strategy and Information Operations, National Defense University, ICAF. Her certifications include OSD Financial Management Level III, ISACA Certified Information Security Manager (CISM), DAU DAWIA, Level II Program Management & IT Level I, FAI Contracting Officer Rep, Level II, NDU, IRM College, Federal Chief Information Officer & National Telecommunications and Information Systems Security

QUESTIONS AND ANSWERS

We have your bio, but what should readers know about you?

I am results oriented. I don't like surprises and I welcome and encourage good ideas. I prefer to rely on research and analysis as the basis for informed decision-making. I continuously look to establish, build, and maintain partnerships to enhance enterprise IT capabilities.

I am also a strong advocate of the CIO's authorities established in law, DOD policies and best practices. This is important because the CIO is the most senior technical advisor in an agency. They are the person that if something goes wrong from a technology perspective, they may be held legally and potentially criminally accountable for what occurs.

The CIO is responsible for ensuring investments made in technologies are sound, and the environment secure. While the OCIO does need to manage all the activities that result from these authorities, they need to have visibility and oversight so they can make informed recommendations when advising senior leadership, and in responding to reporting requirements from DOD, the Office of Management and Budget and Congress.

What brought you to DCSA and this position?

I believed I had the breadth of experience and skills to both lead our diverse group of IT professionals and to bring about change through delivery of improved capabilities and services. Being on the job now just over nine months, I feel I made the right decision and that the teams are moving in the right direction.

What is the biggest challenge facing the OCIO?

There are several challenges. One is herding the cats. Our network and asset management operations are distributed, and the DCSA workforce is accustomed to working with limited coordination and collaboration. Clearly there are network performance issues and application latency concerns. I am partnering vertically and horizontally to change this dynamic to reduce redundancy and inefficiency.

A key component is educating the workforce on the complexity of IT environment. Most people don't understand that DCSA does not manage all aspects of our network or applications; there are many players. For instance, the Defense Information Systems Agency (DISA), U.S. Marine Corps G6, the Office of Personnel Management (OPM) and all military installations affiliated with the DCSA network have equity. At the Russell-Knox Building, the Naval Criminal Investigative Service Information Technology Common Services Unit (ITCSU) plays a role in network services provided into the building.

I encourage everyone to take an active role in helping us identify issues and or concerns by submitting timely and accurate trouble tickets and responding to the technical team queries. Your input facilitates their troubleshooting methodologies to address your concerns and remove obstacles to performance. Often people either forget to submit helpdesk tickets when they have challenges, open tickets but then never get back to the technician to help troubleshoot and resolve the problem, and depending on the problem, we must bring in third parties to assist. Please make yourself available to the technical team to assist in determining the root cause of the helpdesk ticket as the causality can be as unique as each user, platform, or application.

Related to that, we are working on an updated OCIO IT service catalog that will enable users to better understand what IT services and equipment are available, how to request capabilities and clear expectations on delivery. The team continues to make progress on developing dashboards that will support greater visibility into OCIO operations and capabilities by location.

All that said, we are doing a lot to help ourselves. We completed a three-pronged approach to addressing network performance and latency that involved on-site support, independent third-party vendors and DISA who are fully engaged on the network circuit outages, the application latency, and the phone issues.

As the new person, I ask a lot of questions to ensure I understand the issues and environment to put forth innovative solutions to meet the agency's evolving needs. I believe partnerships are critical, so as the CIO, I engage the leadership within DCSA, DISA and my DOD counterparts weekly to address IT issues. OCIO leaders conducted a site visit in December, to codify and maintain enduring relationships between our organizations.

DCSA recently passed a Command Cyber Readiness Inspection by DISA. How significant is that? What does that mean for the agency?

The Command Cyber Readiness Inspection (CCRI) program is a thorough audit of the agency's cyber posture to determine risk and security of data and systems. It determines an agency's cyber authority, critical to the protection of the DOD networks for NIPRNet, SIPRNet, and Cloud systems/enclaves/data risks to the DOD. The inspection is conducted by certified DOD teams under the direction and authority of U.S. Cyber Command and Joint Forces Headquarters - Department of Defense Information Network (JFHQ-DODIN). DCSA scored in the "Low Risk" range, the first agency within the DOD to score this under the new criteria. It is a monumental achievement that demonstrates our cybersecurity excellence through continuous security efforts including self-assessments that continue to improve the agency's effectiveness and efficiencies when facing new and emerging threats. .

Technology changes very rapidly. How do you balance the day-to-day IT needs of the agency with the need to look to the future for upgrades and enhancements?

We are engaged in this balancing act every day. Before we spend $1 of taxpayer resources, we want to ensure that the investments we're making will not only support what we are doing today but can also be leveraged towards where we need to go in the future. We are putting in place processes to support IT Capital Planning and Investment Control (CPIC) as well as processes to meet DOD Policy for IT Spend Certification of Funds. These are new process to DCSA under the OCIO portfolio in FY24.

Can you talk about the agency's plans for ICAM and Zero Trust initiatives?

ZeroTrust (ZT) is a DOD mandated framework which illustrates no implicit trust granted to assets or user accounts. This mandate directs full operational capability by FY27. ZT is set to address cyber threats and attacks that are evolving at an ever-increasing pace and requiring a coordinated, defensive response that is adaptive, flexible, and agile. Currently, DCSA is in the beginning stages of the ZT journey. We have conducted an enterprise wide ZT capabilities assessment to document the current state for long term adoption of ZT solutions. The first of the seven pillars of ZT will be stood up in FY24.

Identity, Credential, and Access Management (ICAM) is a set of tools, policies, and systems used to enable the right individual to access the right resource, at the right time, for the right reason and is foundational to attain a Zero Trust ecosystem. ICAM encompasses the full range of activities related to the creation of digital identities and maintenance of associated attributes, credential issuance for person/non-person entities, authentication, and access management control decisions based on authenticated identities and associated attributes. All of this means that a person's identity is intended to be verified and validated continuously in the background as they traverse the network, systems and data ensuring that they have the appropriate access before being given access through a single sign-on process.

Our goal in the short term is to adopt enterprise solutions for DCSA systems that prevent unauthorized access to data and services in real-time through context-aware access control, leveraging automated risk decision points that incorporate system, applications, user, networks, endpoints, and data. In this manner, our ZT architecture will shift from a location-centric network access model to a data-centric approach enforcing fine-grained security controls between users, systems, data, and assets that change over time.

What other changes are on the horizon for IT at DCSA?

I think it's important that instead of addressing changes on the horizon, to focus on the priorities for DCSA; and there are many. For instance, we are reengineering the network to meet DOD ZT architecture frameworks. We are ensuring we provide IT capabilities that are tailored to the unique personas in the mission elements and mission enablers.

From a user perspective we are looking at this from the perspective of what does a user need to be effective in the performance of their duties when it comes to technology. Do they need a laptop or a desktop? If their duties do not allow for telework, maybe a desktop makes more sense. Do they travel regularly in the performance of their duties? If so, they may need something light weight, that can also double as a tablet to minimize the number of devices they need to carry and that we need to keep secure and support. How many monitors do they need? Our cell phone contracts are up for recompete. Do we need more cell phones, or do we need to enable Jabber on computers so that the laptop now also acts as the phone? These are just a few examples of things we are discussing with mission areas to develop user personas.

I also want to create an IT environment that facilities the development and maturation of analytics as well as Artificial Intelligence and Machine Learning. In other words, how do we take all the agency initiatives that we are currently working and develop integrated enterprise solutions

In closing, what is one thing about the OCIO that the DCSA workforce should know about the team and your priorities that they may not know?

The DCSA CyberWorkforce implementation plan for DOD 8140 will be in full effect on Jan. 1, 2024. This is a transition from the DOD 8570 set of standards. The CyberWorkforce implementation plan will ensure the identification, tracking, and reporting of DOD cyberspace positions and is the foundation for developing enterprise baseline cyberspace workforce qualifications.

DOD 8140 was built to unify the cyber workforce, establish a common data model with the DOD Cyberspace Workforce Framework and to enhance cyber mission readiness across the DOD. The Program outlines qualification standards and requirements for each work role according to three levels of proficiency while providing flexibility for enterprise implementation and individual career path development. It professionalizes the DCSA IT workforce, which in turn provides the agency with the best qualified IT technicians.

New Personnel, Support and Collaboration Transforms DCSA Field Operations

By John Joyce
Office of Communications and Congressional Affairs

Perspectives from the Western Regional Summit

SAN DIEGO – Defense Counterintelligence and Security Agency (DCSA) Western Regional Director Zia Neblett reflected on the transformation of DCSA Field Operations since the agency's reorganization into Western, Central, Eastern and Mid-Atlantic regions in 2022, consolidating background investigations, counterintelligence and industrial security field personnel under one management structure.

She shared her perspective regarding an influx of new personnel and mission support coupled with leadership visits and two regional summits held in August 2023 — the Western Regional Summit followed by the Central Regional Summit.

"There's nothing like in person face-to-face contact," said Neblett. "I've seen how the workforce interacts, engages and responds to leadership engagements and they really appreciated that support at our first summit in San Diego. They actually saw leaders in the field coming out to hear their concerns, – to talk with them about what we're doing while trying to alleviate some of the issues that the field has had for a very long time."

Future summits and ongoing in-person engagements are anticipated as DCSA and regional headquarters communicate with increased transparency to the field through consistent and clear command and control guidance.

A panel of agency subject matter experts prepare to answer questions of the attendees of the Western Region Summit.

Alex Rivera, Human Capital Management Office, outlines the various opportunities available through the Employee & Leader Development program during the Central Regional Summit.

This guidance, – outlined in the Field Operations Command and Control Structure manual issued in August 2023, – describes a matrixed structure in which Mission Support, Field Operations, and Mission Elements report to DCSA leadership, promoting and encouraging collaboration and communication across the different functions.

"The beauty of collaboration, especially in-person events and meetings, was seen by all at the summit," said Neblett. "It was the first time we had all those leaders in the same place, hearing the same message, and having the opportunity to talk to all of the mission support elements at the same time — level set on what's important and how to execute."

The unified message communicated at the Western Region Summit: "DCSA is integrating across all missions to operate as a single, unified Gatekeeper culture."

"To create a better everyday experience for field operations workforce that reflects and encourages deliberatively collaborative and coordinated mission activities and improved access to resources and functional support" is Neblett's

Mid-Atlantic Regional Director Justin Walsh (left); Eastern Regional Director Dr. Gregory Estevez; and Western Regional Director Zia Neblett attend the Central Region Summit.

Assistant Director of Field Operations Larry Vincent clarifies a point during the Central Region Summit.

vision for the Western Region, and reflective of what each DCSA regional director envisions for Field Operations in their respective regions.

Perspectives from the Central Regional Summit

Central Regional Director Roy Hawkins described the agency's outlook on Field Operations while speaking to his audience at the Central Regional Summit, which focused on unifying DCSA culture, purpose and efforts for greater impact on national security.

The Aug. 29-31 Central Regional Summit – featuring opportunities to network among those who met in person for the first time coupled with information updates, – fostered unity of effort regarding myriad programs such as professional development opportunities for employees.

Hawkins emphasized that he emulated highlights and best practices applied at the Western Regional Summit held three weeks earlier when Neblett led the first DCSA regional summit under the Field Operations Directorate.

"The participation of the regional directors is an effort to ensure standardization as we all work to understand the challenges and pain points across the field and share best practices and lessons learned," Neblett explained while attending the Central Regional Summit.

"There was so much positive energy while we actually brought teams together across the mission, across our region, and across four regional directors with some of their mission leads," said Hawkins. "We talked about Gatekeeper culture and our strategic plans to operate as a more agile team with precision for an even greater impact on our missions and services."

The challenges, according to Hawkins, were daunting as he looked at a map displaying the vast panorama of DCSA's Central Region encompassing 21 states and 600 employees working at over 50 offices.

"That's the backdrop to the four missions spanning across our region," said Hawkins, former unit chief for the FBI's Foreign Threat Tracking Task Force, who has travelled from the Central Region's Irving, Texas field office to meet and engage with employees based in Michigan, Minnesota, Mississippi and Oklahoma.

"In addition to fostering our common DCSA culture, we are creating a shared perspective of goals and objectives — an environment of shared ownership for success," he said. "We are also working to effectively leverage and synchronize the unique capabilities of each of the four missions to function with greater speed, precision and impact. That's a challenge in the context of our geographical expanse — 1.3 million square miles. The challenge is also communication. We must communicate early, often and consistently. It's got to go up, down and lateral. It requires robust engagement and timely information sharing across a large landscape with that many people with technology. At the same time, – everything can't be done on Teams, – we have to get in front of people. Some things must be in person with people in the same room and that's why this summit was so important."

Hawkins anticipates that "unintended and tertiary effects" will spread across DCSA's regions as a direct result of Western and Central Regional Summit in-person meetings, collaboration and networking.

"There's so much energy and we don't even realize what's going to happen," he said. "I received calls from background investigator SACs (Special Agents in Charge)

Central Regional Director Roy Hawkins provides opening remarks for the Central Region Summit.

asking me to come to the Kansas City area of responsibility — the second largest footprint of my background investigation workforce — to discuss their perspective on how they can work better with counterintelligence teams. So, they're driving that conversation and that's what I mean by creating an environment where people take shared ownership. Now they are taking ownership and helping me to build robust ownership."

Moreover, Field Operations leaders and supervisors in attendance at both regional summits took ownership while collaborating on field operations guidance and best practices for potential integration across regions. In addition, they examined continuous process improvement and the application of business process re-engineering practices to work collectively as a single agency.

Foundational Field Operations Guidance

The Field Operations Command and Control guidance describes in detail how the new Field Operations structure makes their vision a reality. It sets the stage for continual collaboration and unity of effort as the agency's different cultures merge into one cohesive organization.

"We've been very successful in laying the foundation for the field while focusing on making sure we had the right structure in place with the right people, relationships and guiding documents," said Larry Vincent, DCSA Assistant Director for Field Operations. "Now, we're close to fully staffed with most of our mission support in place and postured to provide better support to the field. We are also on the cusp of opening our first regional headquarters — Dallas Farmers Branch — in February 2024. It will be the first headquarters designed with the new field concept in mind. All regional directors and mission directors will be under one roof with a regional director."

Vincent cites four lines of effort under DCSA's Field Operations umbrella where mission headquarters and mission support personnel work in coordination and collaboration as a team in a matrixed structure to:

- Standardize administrative policies and operations across the missions and regions.
- Drive mission integration with the regional structure.
- Improve communication between headquarters (national and regional) and the field.
- Increase responsiveness of mission support to the field.

"We're staying focused on the fundamentals," he said. "I am extremely focused on how well we do mission integration across our regions and across our missions. It's important for counterintelligence and background investigations to work with each other in support of DCSA's mission as we deliver a standard product across the country."

Moreover, first line leaders and employees across the four regions have dedicated and responsive points of contact in the Security Program Office, Chief Information Office, Logistics Management Office, Diversity and Equal Opportunity and the Human Capital Management Office who they personally know through frequent site visits. Consequently, the workforce is becoming more streamlined and proactively engaged on issues and processes to better support the field.

Transformation in Culture, Organization and Management

"Field transformation has made significant progress in the last year. I am extremely proud of how far we have come and where we are going. With each passing month since transformation began, you can see that real progress is being made to build one DCSA culture. Mission support personnel have been forward deployed to the regions and that support has continued to grow," said DCSA Mid-Atlantic Regional Director Justin Walsh. "Within the Mid-Atlantic region, significant progress has been made on integrating the field missions and we have proven success with numerous high impact case studies and examples. These wins on integration are important, because they serve as a model that can be used to build processes resulting in operating procedures that allow integration to occur routinely in full compliance with policy, law and regulations."

Walsh continued, "The wins also show employees how their actions within their mission can impact other missions and have an even greater impact on national security. In fiscal year 2024, Field Operations is committed to expanding integration even further and continuing to build and improve Gatekeeper culture."

DCSA Eastern Regional Director Dr. Gregory Estevez compared the transformation and integration taking place throughout DCSA as the perfect example of business transformation as defined in a 2022 TechTarget.com report by George Lawton, called 'The Evolving CIO Role: From IT Operator to Business Strategist.' The report describes the term as a description of what happens when an organization makes fundamental changes on how it operates, with an overall aim of fully enhancing operational performance.

"Eastern Region experienced positive transformational changes in its culture, organization and management structure," said Estevez. "These changes have directly increased the efficiency and effectiveness of Gatekeepers in the region, by allowing our teams in the field to achieve and surpass operational performance objectives."

Direct Mission Support to the Field

A key concept of mission support to Field Operations is defined as "direct support." DCSA Mission Support headquarters dedicates specific personnel from their staff, – known as mission support elements, – to provide direct support to each of the four DCSA regions and leadership. The Mission Support Elements are authorized to respond directly to field personnel requirements and requests for assistance.

"The overarching benefit and manifestation of the Field Operations implementation is what I call leadership presence. Senior executive leaders are embedded in the field as the voice of the regions for the first time," said Hawkins. "With the Field Operations construct fully implemented, I see buy-in and great teamwork from the mission managers and the 500-plus DCSA mission and mission support subject matter experts. For the Central region, I observed our teams deployed in various locations, from the U.S.-Mexico southern border to the Canadian border focused on the mission. As regional director, my focus is to ensure the mission teams are equipped to move out to their jobs, and to remove obstacles that prevent them from performing their mission."

Changing Role of the Regional Directors

In short, the focus and energy of DCSA's regional directors involve managing the implementation of strategic initiatives, driving integration across missions and regions, managing key personnel actions within their respective regions, and ensuring effective mission support to field personnel. They are responsible for effective communication between the field and Field Operations headquarters.

DCSA Inspector General Philip Kroop (center) answers questions after his presentation at the Central Region Summit.

As Vincent directs Field Operations, – Neblett, Walsh, Estevez and Hawkins, in collaboration with mission headquarters, are engaged in their regions to drive mission success while ensuring consistent execution of DCSA-wide and cross-regional policies and procedures across Field Operations equities. They also collaborate to establish aligned and integrated processes in coordination with regional mission directors to determine, monitor and analyze field-wide goals, metrics and reporting.

They ensure ongoing mission integration and unity of effort in their regions by fostering improved communication related to all aspects of Field Operations in collaboration with Vincent, the regional mission directors, and mission headquarters to further unity of effort across regions and missions.

What's more, the four regional directors constantly work to enable cross-mission and cross-region integration where missions overlap. They encourage mission integration through cross-training, information sharing procedures and detail opportunities. Consequently, mission support elements in the field are improving support to DCSA employees in the regions to ensure mission success.

"It's a culture change. Everyone's getting accustomed to a new way of doing business," said Vincent. "For example, an industrial security representative who may experience a major issue or situation in the field will now go through Field Operations for the resolution. We're very invested in our new Field Operations construct and business rules. It's about relationships, integration and standardizing — all very important."

The importance includes quality of life and work in the field, which goes beyond mission support to risk management and safety.

"We're working on the safety of our agents in the field," said Vincent. He described situations that background investigators may encounter while conducting a residential check and encounters industrial security representatives could face while walking into a facility to check on a network where a cell phone is not permitted.

"We will apply good risk management for our operations in the field while focusing on investigator and agent safety in addition to our foundational lines of effort in fiscal year 2024," said Vincent.

Field Operations communication resources range from Vincent's podcasts to the monthly Dispatch newsletter available in the Field Operations 365 SharePoint page. The directorate provides in-depth resources on its intranet page such as the manual on its Command-and-Control Structure in addition to the Field Operations resource guide, – a handbook for DCSA Field Operations personnel to obtain guidance and support, – that ensures uniform alignment to agency processes across regions and missions in order to improve responsiveness of mission support and transparency of processes.

DCSA Demonstrates New NBIS System to Thousands of Federal and Industry Partners

By John J. Joyce
Office of Communications and Congressional Affairs

QUANTICO, Va. – The National Background Investigation Services (NBIS) Training Office provided a system demonstration to thousands of NBIS users and stakeholders during the latest NBIS Demo Day hosted by the Defense Counterintelligence and Security Agency (DCSA).

More than 5,300 participants from federal agencies and industry attended the virtual demonstration held in the wake of their transition from using Electronic Questionnaires for Investigations Processing (eQIP) to NBIS Agency for case initiation and eApp for the subject's submission of standard investigative forms.

The 10th NBIS Demo Day held on Nov. 1 primarily focused on subject management, eApp and available NBIS training resources.

"NBIS Demo Day attendance nearly tripled in size since the onset of our training sessions," said Scott DiStefano, NBIS Training chief, adding that the session was interactive with participant questions answered by NBIS experts in real time via the Teams' chat function. "Our representatives from NBIS Training, Solutions, eApp, and Onboarding teams fielded over 1,000 questions from the audience and customers."

The session specifically included an NBIS status update, a system demo, information on development, and discussion on NBIS features and capabilities focused on Release 4.5.

"Since being stood up in 2020, the NBIS Training program provided live training to more than 6,000 users through over 200 live webinars and crafted over 135 training products that include eLearning modules, job aids, knowledge articles, micro-learnings, and video presentations," said DiStefano. "The NBIS Training program also developed a suite of eLearning options that recorded over 50,000 course completions to date. By thoroughly understanding stakeholder and user needs and adeptly adapting to NBIS Agile processes and the evolving Personnel Security Enterprise, the NBIS Training program achieved remarkable success in a rapidly changing environment."

NBIS Demo Day presenters ensured that federal and cleared industry stakeholders and users — including applicants, reviewers and approvers — have the necessary knowledge, including the latest updates, to successfully initiate and submit investigative forms and requests through the new NBIS Agency and eApp system.

"Thank you for all of your hard work, scaling efforts, user management training and continued partnership as we transition out of eQIP into eApp," Sarah Souza, NBIS Planning and Deployment Office lead, told the NBIS Demo Day audience. "We will continue in reference to eApp and NBIS Agency to make enhancements and add additional functionality as well as resolve any issues that we are made aware of in production."

For applicants, eApp provides a single-page solution based on modern and simple design elements, making the standard form completion process intuitive and easier to use. For agency and industry users, NBIS Agency provides robust form review logic, substantially reducing error rate once eApp is submitted and returned to agency for review.

NBIS Agency is the new application allowing security managers and facility security officers to submit case requests for background investigation and manage subjects throughout the personnel vetting process.

NBIS Demo Day concluded with a tour and overview of training resources available to customers via the Security Training, Education, and Professionalization Portal (STEPP).

"We're accommodating different styles of learning," said LaShundra Billups, NBIS Program analyst. "If you prefer to hear a casual conversation as we discuss NBIS topics, you have the capability of clicking and listening to the podcast series."

In addition to podcasts, STEPP provides training for all NBIS users. The STEPP platform consists of NBIS education webinars, micro-learnings, job aides, knowledge articles, and video products covering shared services, workflows and configurations as well as materials supporting federal and industry onboarding, scaling and operationalization of NBIS.

To access the NBIS training via STEPP, go to: https://cdse.usalearning.gov/.

DCSA renames Counterintelligence Award

By Beth Alber
Office of Communications and Congressional Affairs

Former DCSA Assistant Director for Counterintelligence and Insider Threat Andrew Lochli (right) and Michael Donnelly, son of John F. "Jack" Donnelly, hold a letter signed by former DCSA Director William Lietzau announcing the renaming of the CI award to the Jack Donnelly Award for Excellence in Counterintelligence during a ceremony on Sept. 12, 2023.

Thirty years after the counterintelligence program was established, DCSA hosted the family of John "Jack" Donnelly, the director of the Defense Investigative Service (DIS) from 1988 to 1996, for a ceremony to rename the DCSA Award for Excellence in Counterintelligence to the Jack Donnelly Award for Excellence in Counterintelligence on Sept. 12, 2023, at the Russell-Knox Building, Quantico, Va. This name change celebrates the 30th anniversary of the counterintelligence program he established in 1993.

Donnelly served in many counterintelligence positions throughout his career, starting with the Naval Investigative Service from 1951 to 1981. He left NIS and entered the Senior Executive Service, serving as the as director for Counterintelligence and Investigative Programs in the Office of the Deputy Under Secretary of Defense for Policy. In 1987, he was elevated to the position of Assistant Deputy Under Secretary of Defense (Counterintelligence and Security).

In 1988, Donnelly was appointed as the director of DIS, where he oversaw the security of cleared defense contractors and security background investigations of industry personnel. During his tenure at DIS, he transformed the agency' relationship with cleared industry to promote partnership and mutual responsibility

History of the DCSA Award for Excellence in Counterintelligence

The award was established by the Defense Security Service, a legacy organization of the Defense Counterintelligence and Security Agency (DCSA), in 2010 to encourage and reward cleared companies that strive to deter, detect, and disrupt the theft of sensitive or classified U.S. information and technology by foreign entities. William Stephens, then Director of Counterintelligence, was the driving force behind the award's creation.

Selection then and now is highly competitive and up to four cleared companies or academic institutions are recognized annually. The Excellence in CI award is intended to encourage highly mature and effective CI programs that enhance national security and promote the uncompromised delivery of sensitive and classified services and capabilities to the Department of Defense (DOD) and other U.S. Government agencies. Reporting by the company needs to demonstrate measurable counterintelligence (CI) results, a solid commitment to CI practices, and cooperation with the DCSA and other U.S. government agencies.

DCSA Acting Director Daniel J. Lecce (right) presents the Jack Donnelly Award for Excellence in Counterintelligence to Texas A&M University and Chancellor John Sharp in the George H.W. Bush Presidential Library and Museum Auditorium, College Station, Texas, on Nov. 6, 2023.

“DCSA is grateful for Director Donnelly’s legacy and his outstanding leadership and vision,”

Ellen Ardrey, DCSA Chief of Staff

DCSA Chief of Staff Ellen Ardrey (far right) presents Terry Donnelly (left), wife of Jack Donnelly, with a DCSA coin, while her son Michael looks on. (DOD photos by Beth Alber, OCCA).

for preserving national security. Under Donnelly’s guidance, the DIS established a program that trained and sensitized investigators to counterintelligence red flags. His dedication to the national security mission led to the establishment of the agency’s counterintelligence mission in 1993.

“DCSA is grateful for Director Donnelly’s legacy and his outstanding leadership and vision,” said Ellen Ardrey, DCSA Chief of Staff, during the ceremony. “DCSA has prospered as a result of the foundation of excellence he established. “His friends and colleagues would remember him as a leader and mentor,” Ardrey continued, “whose dedicated work contributed to national security and whose guidance, caring and wit positively impacted many.”

Attending the event were family members of Donnelly to include his wife Therese “Terry” Marie Donnelly. “If my father were here, he’d acknowledge the contributions of the agents and support staff,” said Michael Donnelly, son of Jack Donnelly. “He always ensured he recognized those supporting the mission.”

DCSA leaders convene with Multinational Industrial Security Working Group to Standardize Security

By John J. Joyce
Office of Communications and Congressional Affairs

Three DCSA Industrial Security Directorate leaders represented the United States at the 38th annual Multinational Industrial Security Working Group (MISWG) Plenary, in Zurich, Switzerland, from Sept. 11-15.

Richard Stahl, Kristy Engholm and Matthew Kitzman attended the MISWG Plenary to oversee and administer agency level guidelines and international responsibilities regarding cleared U.S. industry's involvement with foreign governments, foreign contractors and NATO on behalf of the Office of the Under Secretary of Defense for Policy.

"The MISWG provides a unique opportunity for the United States to further build on those relationships with 36 plus partner nations and a forum to shape the face of industrial security globally to further enhance our national security as we move into the future," said Stahl, DCSA International and Special Programs Operations chief.

The MISWG, – created in 1986 as an informal non-governmental body, – develops common security practices and procedures for the protection of classified information shared under non-NATO Multinational Defense Programs and international industrial security matters. It is comprised of NATO member nations (except Iceland), as well as Australia, Austria, Finland, Israel, Sweden and Switzerland.

Stahl, Engholm, Kitzman and their international counterparts convened at the forum to discuss ways to adapt security practices to continuing changes in the overall security environment, defense industry trends and international industrial security.

"There are 104 participants from 36 country members in attendance," said Stahl, adding that, "one country is participating as a guest and one as an observer."

The MISWG mission is to promote, improve and harmonize common international industrial security best practices to safeguard classified and certain other forms of government-controlled information in order to confront current and emerging security threats and challenges within its scope.

ZURICH, Switzerland (Sept. 14, 2023) – DCSA International and Special Programs Operations Chief Richard Stahl confers with his counterpart from the Netherlands about an issue related to the Multinational Industrial Security Working Group (MISWG) mission that promotes, improves and harmonizes common international industrial security best practices to safeguard classified and certain other forms of government-controlled information in order to confront current and emerging security threats and challenges within its scope.

ZURICH, Switzerland (Sept. 14, 2023) – DCSA International and Special Programs Operations Chief Richard Stahl, left, discusses a Multinational Industrial Security Working Group (MISWG) issue with his counterparts from the United Kingdom and the Netherlands.

Industry Day goal to identify system to update National Industrial Security System

By Jessica Thomson
Program Executive Office

As part of the development of a modern, single system to replace the National Industrial Security System (NISS), the Defense Counterintelligence and Security Agency (DCSA) hosted an Industry Day for NISS Increment 2 (NI2) on Sept. 26-27, 2023.

The Industry Day provided an opportunity to collaborate with industry partners, share information, and gather market research in support of the development of NI2. The NI2 mission is to incorporate the state of the technology of the industrial security mission with other DOD/DCSA mission areas, government data sets, and commercial/open-source data sets. NI2 will replace NISS legacy systems and applications with a modernized enterprise level capability single NISS system in a secure and resilient cloud while also maximizing reuse of DCSA information technology investments to reduce lifecycle costs.

Industry Day began with keynote speeches by Jeffrey Smith, former DCSA Program Executive Officer (PEO), who discussed DCSA's vision as America's Gatekeeper and the importance of national security to our mission. Smith highlighted NI2's role in the Vetting Operating Model that establishes a set of design principles that shift the agency from manual to automated processes; from compliance-based to risk-based operations; from siloed organizations to integrated organizations; ad hoc to standardized services; and resource-intensive to requirement-driven method; and from agency-centric to customer-centric.

Additionally, Gus Greene of the DCSA Industrial Security Directorate discussed the four missions of DCSA including Personnel Security, Counterintelligence and Insider Threat and Security Training. David Drys, DCSA PEO program manager, National Security Systems (PM NISS), discussed NISS's mission, current capabilities, NI2's vision and program objectives.

Drys was encouraged by the successful event. "I was very impressed with the amount of interested companies and the scope of participation from both large commonly known firms to smaller more boutique companies I had never heard of or worked with before," he said. "The depth of the questions asked during the one-on-one discussions has me very excited to see the innovated solutions that will be brought forth to support the development of the next generation NI2 system for industrial security."

Industry Day was an exciting opportunity to collaborate with mission partners, and the agency shared and received positive feedback and valuable information from those who attended. In wrapping up the event, PM NISS held one on one meetings with interested partners who then were invited to submit white papers.

DCSA Industrial Security Leaders Inspired by George Washington's Wisdom at Mt. Vernon Event

By John J. Joyce
Office of Communications and Congressional Affairs

MT. VERNON, Va. – Retired Marine Corps Gen. John Allen looked at Continental Army soldiers marching to their Valley Forge winter encampment and as he pointed them out, Defense Counterintelligence and Security Agency (DCSA) industrial security leaders surveyed the scene that took place on Dec. 19, 1777.

It was a turning point in DCSA employee discussions with Allen about strategic leadership in the context of George Washington's philosophy and experience during the Industrial Security Senior Leadership Annual Meeting (IS SLAM).

Retired Marine Corps Gen. John Allen (left), former commander of the NATO International Security Assistance Force and U.S. Forces in Afghanistan, speaks to the DCSA Industrial Security Senior Leadership Annual Meeting (IS SLAM) participants at Mount Vernon, Va., Sept. 23, 2023. (DOD photos by John Joyce)

"Here he is at Valley Forge," said Allen, as all eyes focused on the iconic Revolutionary War painting. "His troops are moving forward in the snow."

Allen, – former commander of the NATO International Security Assistance Force and U.S. Forces in Afghanistan from July 2011 to February 2013, – also alluded to his personal leadership, lessons and experience in combat while serving in Bosnia, Iraq and Afghanistan during his remarks.

"I spent the first 15 years of my time in the Marine Corps on a cold weather mission," said Allen. "Well, I've been cold and look at this painting and get cold in a second watching it. There's two things that are really important here. This army is suffering from an absence of resources. It's not entirely clear it's going to survive the winter much less survive the British. There's George Washington right alongside. Leaders have to be present with their troops."

The Importance of Integrating Strategy, Leadership and Management
GOOD STRATEGY + GOOD LEADERSHIP + GOOD MANAGEMENT = SUCCESS
LEADERSHIP • INSTITUTE

DCSA Industrial Security Senior Leadership Annual Meeting (IS SLAM) participants learn about strategic leadership in the context of George Washington's philosophy and experience.

DCSA Acting Director Daniel Lecce, – serving as deputy director while speaking to IS SLAM attendees at the agency's Quantico headquarters, – conveyed a similar message as he kicked off the event on Aug. 28 that continued at the Washington Presidential Library's Rubenstein Leadership Hall in Mt. Vernon, Va., over the next two days.

"People are our greatest mission," Lecce told DCSA Industrial Security Directorate leaders, supervisors and Field Regional Mission directors while emphasizing culture and unity of effort. "It's incumbent on us to recognize, foster and encourage our workforce."

IS SLAM participants engaged with multiple Washington Presidential Library speakers who focused their Mt. Vernon briefings on the tenets of civility, ethics, integrity and credibility in leadership and decision-making as evidenced by George Washington throughout his life.

"You live in a world that's enormously complex today," said Allen while addressing IS SLAM. "It's not only a multi-domain environment within which you are attempting to defend our industrial base and our security, but we have enemies out there operating against us 24 hours a day - whether it's the Russians, Chinese, Iranians or the North Koreans or any number of smaller terrorist organizations attempting to penetrate our security membrane. It's a complex organization and it's not just complex in that enemy-threat context, it's complex in how you are organized and how you are distributed. You are hierarchically organized. You are geographically distributed. You have multiple different kinds of subordinate missions and all of that can only be pulled together by strategic leadership in a sense and an understanding that strategic leadership is vitally important. George Washington really set the conditions for us to understand that."

The importance of the conditions and character demonstrated by Washington 250 years ago that are relevant to today's leadership was paramount in discussions on the characteristics and components of character taking into consideration the relationship of character, integrity and trust.

IS SLAM participants discussed how Washington's strategic vision and collaboration with different teams resulted in the best possible outcome, changing the course of history: military (Washington—Rochambeau decision to attack Yorktown), legislative (Constitution and the Bill of Rights) and political (Washington D.C. – newly formed Bank of the United States) in addition to Washington's "quiet" collaboration (daily dinners during the Constitutional Convention).

They also studied U.S. founding fathers to include Alexandar Hamilton's strategic approach to the nation's first financial crisis, – known as the Panic of 1792 in the wake of Wall Street's first crash in late 1791, – as an example of analytical and operational leadership while managing an acute crisis.

Upon the in-depth study and discussion of Washington's life and leadership, the IS leaders report that in all cases since the founding of the United States, successful leadership requires understanding and trust. Moreover, they can point to myriad historical and modern-day examples that prove character, integrity and effective communication are vital to success.

IS SLAM also featured remarks by Matthew Redding, DCSA assistant director for Industrial Security, followed by briefings from leadership focused on topics that included field operations, counterintelligence, the National Industrial Security System, the NISP, and DCSA Industrial Security operational goals.

Pennsylvania Community Honors the Patriotism and Sacrifice of DCSA Employee's Uncle at Football Stadium Dedication ceremony

By John J. Joyce
Office of Communications and Congressional Affairs

WEST SUNBURY, Pa. – Chad Plesakov looked upon the Moniteau High School football field and reflected on the life of a man who inspired him to become a civil servant at the Office of Personnel Management (OPM) in 1999.

More than a thousand local residents joined him to honor the life of his uncle, Luciano Plesakov, at a Sept. 15 ceremony held at the football stadium.

Chad – currently a Defense Counterintelligence and Security Agency (DCSA) National Background Investigation Services program analyst – recounted his decision to serve his country like his uncle, whose name is now displayed above the stadium's scoreboard as the facility's new name: Luciano Plesakov Stadium.

Luciano, a Moniteau High School scholar and standout athlete, was killed in action in 1967 while serving as a 19-year-old corporal and machine gunner in the Vietnam War. Known for his values, character and leadership, the football and track and field star looked forward to becoming a U.S. citizen after the war.

"My father went through a lot losing his brother, Luciano, and I didn't want him to worry about me," said Plesakov about his decision for not volunteering to serve in the armed forces. "I believed it was the right decision at the time, but it became my biggest regret in life – not serving in the military. Then again, I did the next big thing and became a public servant in the federal government in something as important as investigations and adjudications to make sure that the proper people get into the government and can stay in the government. That's how my uncle's life impacted me, and Luciano impacted the lives of many others to this day. It all leads back to who he was."

Luciano Plesakov, a Moniteau High School graduate known for his values, character and leadership, is pictured with another student sometime in 1964 or 1965.

Chad – among Plesakov family members attending the ceremony held before a football game – watched as the Moniteau school board, faculty, students and community officially dedicated the sports arena in honor of the 1965 graduate, the only Moniteau High School alumni killed in action.

Luciano influenced those who knew him and many who did not know him, including his nephew, Chad, born years after his uncle was killed in action serving his country with the promise that he would be granted American citizenship.

Over the years, Chad got to know his uncle through conversations with family members and those who taught,

> “Luciano impacted the lives of many others to this day. It all leads back to who he was.
>
> *– Chad Plesakov*”

Chad Plesakov addresses more than a thousand local residents who joined him at a ceremony officially dedicating and renaming the Moniteau High School football stadium to Luciano Plesakov Stadium in honor of his uncle, Luciano Plesakov – a Moniteau High School graduate known for his values, character and leadership. Luciano was killed in action as a 19-year-old corporal and machine gunner in the Vietnam War.

coached or attended school with Luciano. He also perused scores of letters sent home from Vietnam.

“Those letters are unbelievable,” Chad told a local reporter as published in a news story in the Explore Clarion guide to Clarion County, Pa., website on Sept. 13, 2023. “It was never about him. It was always about comforting his family. He went because he wanted to end the war and he hated communism because my grandfather hated communism.”

The Explore Clarion article emphasized that Chad’s grandfather, Vasili, had good reason to despise communism, stating that as a Soviet Union army interpreter in World War II, Vasili was captured. At the time, one of Soviet Premier Joseph Stalin’s edicts mandated that any Soviet soldier who was captured rather than fighting to the death would be killed along with the soldier’s family upon returning home.

Consequently, Chad’s grandfather did not return to his home in Russia. “His family and the Soviet military probably assumed that he died,” said Chad, adding that Vasili didn’t want to risk anything by letting his family in Russia know that he was alive.

“He met my grandmother, Ines, in Italy. They got married and Luciano was born there,” said Chad. “Italy was decimated, so they applied and were subsequently granted status as stateless refugees through the U.S. State Department. They came over here to western

Twenty-two recipients of an award presented to them in Luciano Plesakov's name when they were high school students unfurl a 40-by-80 foot U.S. flag at a ceremony on the football field. They were among a thousand local residents and visitors in attendance for the dedication and renaming of the Moniteau High School football stadium to Luciano Plesakov Stadium in honor of Luciano who was killed in action as a 19-year-old corporal and machine gunner in the Vietnam War.

Pennsylvania and the Catholic Church helped them get settled with employment. They eventually bought a farm located in the Moniteau school district. Since then, our family, the Plesakovs, have always been extremely grateful for this country and our freedoms. We're patriotic Americans and I'm sure patriotism and gratefulness was in Luciano's mind when he volunteered to fight in Vietnam against communism."

After the dedication ceremony and the football game was over, Chad continued to reflect on the influence of his uncle on his life and the lives of many others.

"I'm involved in the community," said Plesakov. "I've been in youth sports, coaching football and baseball players and I'm now the president of our girls' high school volleyball program. It's just giving back to the community and showing the character that my uncle had. He was always helping others like that. Character is a big part of his story – the number one thing. If you talk to anybody, they'll say he had the highest character of anybody they ever met."

Letters sent home from Luciano, the first rub from his name on the Vietnam Veterans Memorial Wall, his dress blues, and his varsity jacket were displayed at the event.

The dedication ceremony also featured 22 recipients of an award presented in his uncle's name to Moniteau High School students demonstrating outstanding character, scholarship and athleticism. The Luciano Plesakov Award has been presented to at least one student each year since 1981.

"It's the highest award a student could get in the high school, which teaches about him and keeps his memory alive," said Chad, who transferred from OPM to the National Background Investigations Bureau in 2016 and DCSA in 2019. "The award honors student -athletes who are leaders with good character and grades. The award winners in attendance held a 40 by 80-foot U.S. flag on the field that night. It was so heartwarming to see them come back and some presenting testimonials to say, 'hey, if it wasn't for this award, I might not have been able to fund my academic goals.' There are more testimonials and comments from students and others in the 'Luciano Plesakov Stadium-Moniteau JR/SR High School' Facebook page – it's so incredible.

Overcoming Challenges and Ensuring Preparedness in the Telework Era

By Mark Cerney
Security Programs Office

As a result of the pandemic, many federal government agencies, including DCSA, and numerous private sector corporations and businesses have successfully incorporated telework into their daily operations. This shift towards teleworking offers flexibility and convenience; however, it also presents unique challenges for leadership and the workforce when it comes to emergency preparedness, personnel accountability, and distributed field operations.

While the adoption of new technologies and tools for remote communication and collaboration presents opportunities for enhancing emergency management strategies, it is important for team members and leadership to address the specific challenges that arise in this telework era.

Challenge 1: Personnel accountability in a dispersed workforce

In a telework environment, it can be challenging for team members and leadership to have real-time knowledge of each other's whereabouts. This poses a problem during emergencies when quick communication and accountability are crucial.

> **Solution:** *To overcome this challenge, team members must be transparent in providing their location and status to their supervisors. Updating calendars with status and location, providing contact information, and keeping it readily accessible are essential practices. This ensures that leadership has the necessary information to locate and communicate with team members during emergencies*.

Challenge 2: Reliance on external sources for information

In a telework environment, the workforce often relies on external sources for information during disaster scenarios. However, there can be a tendency to seek information from multiple sources, leading to confusion and potential friction.

> **Solution:** To *address this challenge, team members should be educated on local hazards in their respective areas, including reliable information sources. This prepares them for potential disasters and enables sound decision-making. Emergency Managers working with leadership can assist in finding local, reliable information sources, negating the often-overwhelming amount of information available in a variety of forums. Additionally, team members should be encouraged to sign up for local emergency alerts to receive real-time warnings.*

Challenge 3: Hazards and preparedness in different locations, including field operations.

Teleworking team members, including those involved in field operations, may face different hazards in their residences and in their field sites. This requires individuals to be aware of local hazards and have plans in place to react effectively.

> **Solution:** *To overcome this challenge, team members should be proactive in understanding the hazards specific to their telework locations and field sites. This includes developing plans for power outages, identifying relocation sites, and building emergency kits for both work and home. Staying connected through local emergency alerts and providing personal contact information to relevant systems enhances safety and communication during emergencies.*

Challenge 4: Transitioning to a culture of preparedness for team members.

Transitioning to a culture of preparedness in a telework environment, including field operations, can be challenging for team members in the enterprise, as participation in virtual training may be lacking due to competing priorities.

> **Solution:** *To address this challenge, it is essential for leadership to emphasize the importance of preparedness and create a culture that prioritizes it among all team members. This can be achieved by incorporating emergency preparedness training into mandatory training programs and offering opportunities for in-person and virtual training sessions that cater to the specific needs of team members in the enterprise. By making preparedness a top priority and providing accessible training resources, team members will be equipped with the necessary knowledge and skills to respond effectively during emergencies.*

While the adoption of telework in the enterprise offers flexibility and convenience, distributed operations present unique leadership challenges. By directly addressing the challenges of personnel accountability, reliance on external sources, geographically unique hazards, and transitioning to a culture of preparedness for team members, both leadership and team members can ensure the safety and success of their teleworking workforce.

Defense Counterintelligence and Security Agency

27130 Telegraph Road
Quantico, Virginia, 22134
DCSA.pa@mail.mil
571-305-6562
www.DCSA.mil