Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper

Volume 3, Issue 1

Agency increases field support, resources to encourage integration, better communication

IN THIS ISSUE

ASK THE LEADERSHIP: LARRY VINCENT

DOD CIO AWARD

UNITY OF EFFORT ROAD SHOW

IN THIS ISSUE

FROM THE DIRECTOR 3

AGENCY INCREASES FIELD SUPPORT, RESOURCES TO ENCOURAGE INTEGRATION, BETTER COMMUNICATION 4

REGIONAL DIRECTORS SPEARHEAD INTEGRATION ACROSS MISSIONS, REGIONS ... 6

ASK THE LEADERSHIP 8

DCSA EMPLOYEES PART OF DOD CIO AWARD WINNING TEAM 11

LEADERSHIP OF PEO CHANGES, PART OF CONTINUED AGENCY TRANSFORMATION 12

AGENCY LEADERSHIP WORKS TO FORGE ONE COHESIVE AGENCY CULTURE 14

DCSA BADGES, CREDENTIALS VALIDATE AGENCY AFFILIATION 16

DCSA BRIEFS INDUSTRY ON STATUS OF NATIONAL BACKGROUND INVESTIGATION SERVICES DEVELOPMENT 18

MULTI-DISCIPLINE DCSA TEAM CONDUCTS FACILITY REVIEW 21

SECURITY PROFESSIONAL EDUCATION DEVELOPMENT (SPĒD) 22

PROGRAM HAS SIX CERTIFICATIONS, THREE CREDENTIALS AVAILABLE 22

MILITARY RESERVISTS ON ACTIVE DUTY ASSIGNMENTS POSITIVELY IMPACT DCSA MISSION 24

AIR FORCE CAREER OF FIRST DIS DIRECTOR RICH WITH INTELLIGENCE, COUNTERINTELLIGENCE ASSIGNMENTS 27

Vol 3 | ISSUE 1

DCSA Gatekeeper

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

FROM THE DIRECTOR

Happy New Year. I would like to wish our government and industry partners a healthy and prosperous 2023. DCSA continues to be an agency undergoing fundamental transformation that began with the agency's creation in 2019. We achieved much in 2022, highlighted by advances in the development and implementation of the National Background Investigation Services and evolution in personnel security in support of Trusted Workforce initiatives such as continuous vetting. 2023 will be another year of tremendous success and transformation of our capabilities as we honor our commitment to be America's Gatekeepers.

In the many opportunities I have to speak with key mission partners, stakeholders, and customers across the enterprise I always highlight the urgent need to combat what I see as a critical threat to our nation's security. Our ability to protect our industrial base and key technologies, and to ensure we deliver a decisive advantage over our adversaries is my top priority heading into 2023. DCSA will transform how we support Industrial Security through enhanced integration of the underlying and complementing aspects of our Counterintelligence, Security Training, and Personnel Security missions.

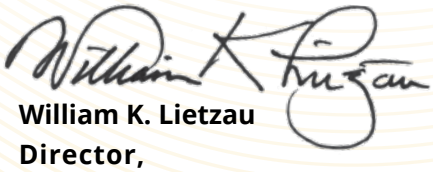
Our January 2022 issue featured our new regional structure and the attending geographic boundaries. The goal with this structural change was to pull DCSA closer to full integration of our mission and to gain efficiencies and effectiveness across the disparate mission elements at the field level where the work for our customers and stakeholders takes place. Since then, we have hired a new Assistant Director, Field Operations, who is featured in this issue. This position is responsible for field resource planning and integration across missions and regions to most effectively support DCSA's overall mission.

We also hired new regional directors whose role is to oversee integrated mission management to streamline and better support critical administrative, logistical, information technology, and information sharing needs across the regions. We have long recognized that the critical work of the agency is done in our dispersed field locations, sometimes under less than ideal conditions. Resolving those issues and putting our field personnel at the forefront of our support is a continuation of the field's transformation.

I recently participated in a change of charter ceremony for the Program Executive Office (PEO), another key transformation effort. In this case, we consolidated several roles and activities presently in the Office of the Chief Information Officer (OCIO), PEO, and Chief Strategy Office into the PEO. A key element of this change is the establishment of an agency Chief Technology Officer or CTO who will lead our thinking on future needs and capabilities.

DCSA is also undergoing internal transformation which should be transparent to our stakeholders. In the fall, the Deputy Director led a Unity of Effort road show to visit our dispersed population to get a pulse of the workforce and to communicate what it means to be the nation's Gatekeeper in today's shifting security environment. This effort directly supports the agency's five-year strategic plan and will help build a unified agency culture. I'm excited to hear the results of these conversations and explore how we incorporate employee feedback into our future efforts.

As we continue our transformation, rest assured that we remain focused on our role as America's Gatekeeper and are committed to delivering the very best personnel and industrial security, counterintelligence, insider threat training products and support to our stakeholders and partners. Thank you for reading and your continued support to DCSA.



William K. Lietzau
Director,
Defense Counterintelligence and Security Agency

Agency increases field support, resources to encourage integration, better communication

By John Joyce
Office of Communications and Congressional Affairs

When background investigators, industrial security representatives and counterintelligence special agents need assistance to successfully accomplish their national security mission, where do they go for support? Who do they contact?

It depends on the requirement but one thing is certain — the Defense Counterintelligence and Security Agency (DCSA) Office of the Chief Information Officer (OCIO), Security Office, and Logistics Management Office (LMO) are engaged to provide increasing security, information technology and logistics support throughout the agency's Eastern, Mid-Atlantic, Central and Western Regions as enabling functions are integrated across mission areas.

"I'm very excited about our increasing support to the field," said Lisa Gearhart, DCSA Security Office senior coordinator for Enterprise Programs. "The more communication, collaboration and capabilities that we can provide to the field through the regional headquarters to empower our personnel and fulfill the mission, the better."

Background investigators, industrial security representatives and counterintelligence special agents in the field are increasingly empowered to execute DCSA's mission as the agency works to standardize administration and operations across missions and regions, standardize mission delivery, and improve communications between headquarters and the field.

Larry Vincent, DCSA's first assistant director for Field Operations, known as the regions' voice at DCSA Headquarters across the missions, inspires enabling support as he promotes integration and standardization across the regions and missions. His voice, which can be heard on monthly podcasts about field support operations via the agency's internal website, advises the regions, including new regional directors who lead the field workforce supporting the counterintelligence, background investigation and industrial security missions.

"The new regional organizational structure under Field Operations is part of our enterprise initiative to integrate DCSA's different missions and cultures into one cohesive organization," said Vincent. "It is driving consistent application of policies related to space, vehicles, supplies, information technology, and general resourcing across the missions. It will also lead to improved mission effectiveness through integration across regions and missions."

The regional directors and Vincent are working closely to increase responsiveness of functional support to the field as they integrate missions and regions while reducing administrative workload on mission leads at headquarters and regional mission directors.

Meanwhile, DCSA's Security Office, OCIO and LMO are coordinating with the Human Capital Management Office and regional directors to hire personnel from government information technology experts to security professionals, filling newly created positions in the regions to provide support and leadership.

"We're pushing out enabling functions to the field," said DCSA Security Programs Chief Edward Fish, pointing out that DCSA hired 11 security professionals, with more new hires pending. Those hired in 2022 to provide security services in the Eastern, Mid-Atlantic, Central and Western regions include specialists in emergency management, physical security, anti-terrorism/force protection and general security.

"We have to understand how our folks plug into the regions," said Fish. "My security folks in the field are supporting regional directors and helping to accomplish their missions but also looking for expertise and direction from headquarters, asking 'how do we do mission assurance and emergency management?' It's also important to establish appropriate command and control relationships with mission and enabling functions, who works for who and who supports who."

In 2022, OCIO hired or was in the process of hiring eight information technology experts, comprising a user experience manager and a user experience analyst in each of the four regions.

"What we've understood from trending issues is that an OCIO person on the ground is able to relay some of the work being done at OCIO to mitigate or triage various issues with IT," said David Jackson, DCSA deputy CIO and User Experience Division chief. "Our user experience managers and analysts physically located with that mission partner have tremendously improved OCIO IT communications in that regional headquarters where they are based. We serve as a bridge between DCSA headquarters and our regional headquarters in understanding how OCIO works, and the expectations and prioritization of things at OCIO. We now have staff in the regions to liaison and socialize processes with key OCIO points of contact."

As the agency's regional organizational structure enhances collaboration in its Field Operations, the Logistics Management Office is looking at ways to consolidate and collocate field

offices in addition to constructing Sensitive Compartmented Information Facilities in the regions.

A case in point regarding the colocation of field offices is the industrial security and background investigation field office in Minneapolis, Minn. The industrial security office is located in the federal building while the background investigations office is located within walking distance at a building five minutes away.

"LMO is providing field support to our background investigation and industrial security customers and we are in the process of posturing to best support an expanding DoD Insider Threat Management and Analysis Center," said Joseph Plesniak, DCSA Field Logistics Support chief. "The on-site presence improves our ability to meet the needs of regional directors as we deliver timely policy and guidance regarding LMO centric programs. Logistical guidance and support to the field — a critical element to the greater mission of the DCSA enterprise — will expand at regional locations as regional locations grow their operations."

How do LMO, OCIO and Security plan to measure success as Field Operations expand under the new organizational structure?

"Success will be measured by our ability to facilitate approved recommendations identified in the Master Space Plan and our ability to provide efficient vehicle support," said Plesniak.

The LMO Master Space Plan for offices and facilities at the regional headquarters outlines support services and innovative yet purposeful, safe and secure spaces that foster a creative, healthy and productive work atmosphere.

OCIO will measure success by gathering and reporting metrics to regional leadership on IT asset deployment, health of IT systems, and any other information technology initiatives impacting access to the DCSA network.

"On the end of any process or request from OCIO, we plan to conduct a follow-up survey to see how the service delivery model worked for the customer, which includes an opportunity to provide recommendations for improvements," said Jackson. "We'll also pull metrics for insights to see how we're performing over a continuum."

OCIO's mission to deliver reliable, sustainable, secure and effective information technology and cyber capabilities to the DCSA workforce — bolstered by increased field support — will prosper in every region, enabling employees to work securely from anywhere as Field Operations continues to expand.

Jackson projects that OCIO priorities will improve performance, increase capacity and build much needed redundancy throughout the regions. Those priorities include the optimization of enterprise information technology cost, programming and execution to improve reliability, performance and network capability; improved workforce development and management; modernized information technology, mission systems and an accelerated cloud adoption; strengthened cybersecurity and prioritized risk management measures; and information technology governance across the agency.

"In this growing environment, there is a number of competing priorities as well as challenges and a set of evolving requirements," said Jackson. "I'm excited to get in the gaps and be someone folks can lean on for understanding IT as an ingest point to folks in OCIO who can help. That's what my mandate is. That's really what user experience is about — being the ingest point and the front door for OCIO and connecting people with a process or an individual that gets them a product or service that they need. We enjoy getting out and meeting folks, and talking to them about their IT specific needs — that's been very enjoyable for sure."

The User Experience Division serves as OCIO's strategic communications partner to improve overall workforce productivity, create a positive OCIO presence, and instill a sense of trust among the agency's user community.

"Once we get established in our standard operating procedures and a good set of metrics, we're going be able to measure more critical tasks than we're doing today," said Fish. "That's one of our objectives for this fiscal year – to surge and finish the standard operating procedures and policies under the DCSA logo to be clear with our objectives for fiscal year 2023. The measurement of effectiveness is something we're going to have to put in place as we build up the structure. Key indicators of success will also depend on feedback from regional directors, employee surveys, and Mr. Vincent himself."

Vincent and DCSA leaders anticipate success via the new regional organizational structure – part of an overarching plan to integrate DCSA's missions and cultures into one cohesive organization – that will lead to improved mission performance through information sharing across mission areas.

As field support increases in synchronization with headquarters and the mission areas, DCSA officials foresee design processes, data strategies and technologies enabling more timely information sharing and the capability to identify what may be hindering integration. Leaders at mission headquarters will support the integration of the mission areas and ensure that mission objectives are carefully aligned to facilitate transparency and data sharing. As field director, Vincent is leading integration across regions and missions with support from mission headquarters, regional directors, and regional mission directors. This cannot be done in a vacuum and must be an inclusive activity throughout DCSA. Transformation of the agency's field organization will help build a Gatekeeper culture in which there is collaboration and synergy across DCSA.

Regional directors spearhead integration across missions, regions

As a part of the field transformation, several new positions were established to include four new regional directors for the Central, Eastern, Mid-Atlantic and Western regions. The role of these regional directors is to oversee administrative, logistics, and cross-mission information sharing across the region. Within their respective regions, they will be responsible for leading the field workforce supporting the counterintelligence, background investigation, and industrial security missions. Working closely with mission headquarters and the assistant director for Field Operations, the regional directors will manage administrative and logistics functions, spearhead integration across missions and regions, and focus on effective communication between the field and headquarters. DCSA has hired three of the four regional directors and what follows is a brief snapshot of these individuals. Hiring is underway for the regional director of the Eastern Region.

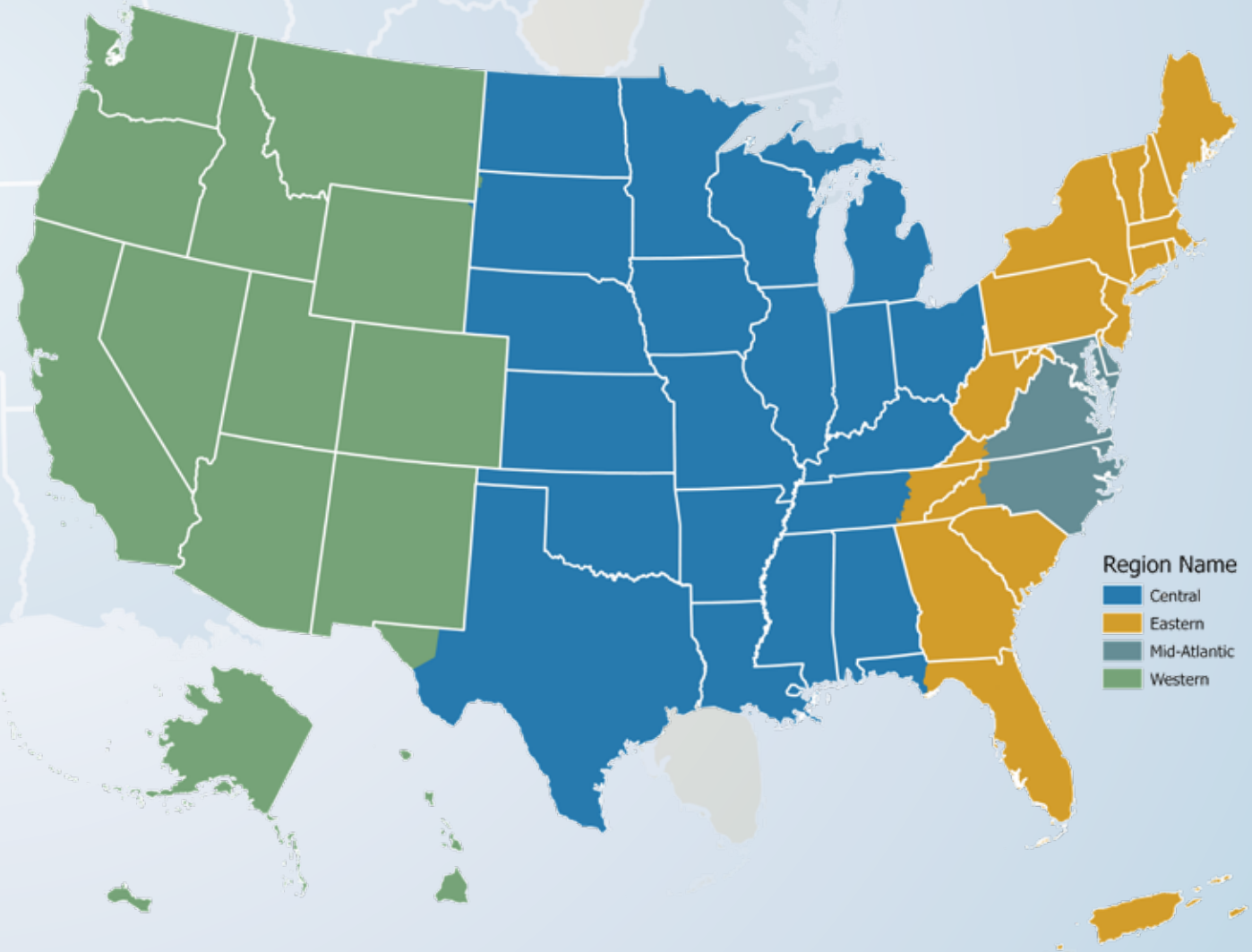
Zia Neblett - selected in October 2022 as a defense intelligence senior level - is the new regional director for the Western Region, based in San Diego, Calif. Previously, she served as the assistant regional mission director for the Background Investigations Field Operation's Western Region. In that role, she provided leadership and supervision for four field offices throughout Greater Los Angeles and San Diego, Calif., and Honolulu, Hawaii. She began her Federal career with the U.S. Department of Transportation, where she served in a number of leadership positions managing a broad range of federal programs and initiatives, to include serving as division chief for the USDOT, Federal Highway Administration (FHWA) Office of Public Affairs providing overall leadership in the day-to-day operation and management of FHWA's public communications program. Neblett's appointment was effective Oct. 23, 2022.

Justin Walsh - selected in October 2022 as a defense intelligence senior level — is the new regional director for the Mid-Atlantic Region, based in Alexandria, Va. While Walsh started his career as a background investigator, he has a long track record of leadership in industrial security. Prior to his selection as the RD, Walsh served as the Regional Mission Director for the Mid-Atlantic Region, where he was responsible for overseeing and partnering with ~3000 cleared defense contractors to protect classified information, critical technologies, and lead operations for eight field offices. He previously served as acting director of Plans and Programs within the Industrial Security Directorate, where he led two distinct functions: Entity Vetting (Facility Clearances, Business Analysis, and Mitigation Strategies) and the Program Management Office (developed and maintained the Directorate strategic plans and managed the associated critical programs and technology). From 2002-2010, he served in a variety of roles to include: Background Investigator, Industrial Security Representative, Foreign Ownership Control or Influence/ International Specialist, and Acting Region Operations Manager. Walsh's appointment was effective Oct. 23, 2022.

Roy Hawkins - selected in October 2022 as a defense intelligence senior level - is the new regional director

for the Central Region, based in Farmer's Branch, Texas. Hawkins joins DCSA from the Federal Bureau of Investigation, where he served as the unit chief for the Foreign Threat Tracking Task Force (FTTTF). His unit was the lead federal agency vetting special interest migrants encountered along the United States borders who posed a national security risk. Before joining the FTTTF, Roy served as the counterintelligence lead supervisor in the FBI Houston field office, where he led intelligence integration between the FBI and Intelligence Community (IC) partners which informed key operational actions to counter foreign adversary activities across the domain. He was also regional program coordinator in support of the South-Central Domestic Director of National Intelligence Representative (DomDNI), an Office of the Director for National Intelligence (ODNI) national initiative. In this capacity, he led actions which brought together the analytical capabilities of eight FBI field offices and many IC partners and fusion centers in five states to address threat issues common across the region. He also brings a wealth of leadership experience from the National Geospatial-Intelligence Agency, the Defense Intelligence Agency, and the Air Force. Hawkins' appointment was effective Dec. 18, 2022.

DCSA REGIONS



ASK THE LEADERSHIP

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

Larry Vincent, Assistant Director, Field Operations

Larry Vincent is the Assistant Director, Field Operations. In this capacity, Mr. Vincent is responsible for field resource planning and integration across missions and regions to most effectively support DCSA's overall mission.

Prior to this, Vincent served as the Executive Officer, DCSA, where he ensured the Director's strategic objectives, goals, and intent for DCSA's organizational climate and priorities are conveyed to DCSA Program Managers and Headquarters Staff Office Chiefs. Before joining DCSA, he was a career naval officer, with 30 years' experience in carrier aviation, requirements, policy and operations.

As an aviator, Vincent accumulated 4,500 hours in three models of the H-60 helicopter with extensive deployments on aircraft carriers in support of operations Restore Hope, Southern Watch, Iraqi Freedom, and Enduring Freedom. He commanded two squadrons, one carrier based, and one forward deployed to Guam. For his final tour in aviation, he led the Navy's MH-60S helicopter wing, geographically dispersed, with 11 squadrons, 130 aircraft and 4000 personnel. In addition to the MH-60S, Vincent brought the MQ-8 Firescout, the Navy's first operational UAV, to IOC.

Vincent's shore duty assignments included tours on the Navy Staff as a requirements officer for all Training Aircraft and on the Joint Staff J-5 as the Division Chief for Strategic Communication and Information Operations policy. He finished his career in the Navy as the Maritime Operations Center Director (MOC-D) for SIXTH Fleet, and Assistant Operations for Naval and Marine Corps Operations in Europe and Africa.

Vincent is a graduate of the U.S. Naval Academy and has Master's Degrees from Auburn University and Industrial College of the Armed Forces.

QUESTIONS AND ANSWERS

We have your biography, but what should readers know about your background?

I moved around a lot as a kid, every two or three years. When I joined the Navy that continued and I found I enjoyed it. I liked being away from the office. I loved deployments and detaching from the carrier; it was important to understand the different mission areas and meet the people executing the mission, whether it was maintenance personnel or those working the helicopter's sonar. It was all interesting to me. And while it's not in my bio, my family is very important — spending time with my family is important.

You've been at DCSA since 2020, what about this job interested you?

When I first came to DCSA in 2020, we were in the middle of COVID and it was hard to get a sense of the organization. I remember my first trip with the Director was to Andover, Massachusetts and the local field office. It was my first time in the field and from that visit, it was clear to me that I didn't understand the intricacies of DCSA's various mission sets. That visit allowed me to get a better sense of the field and the work they were doing; these professionals across the country contributing in so many different ways to the broader DCSA mission. I appreciate the challenges of the field; communicating effectively with the headquarters staff and getting the tools and resources necessary to execute the mission. So, when I saw this job developing, I felt my experience and knowledge of DCSA would be a great fit for the position.

The Director has made a focus on the field a priority. What was his guidance or direction to you in taking this job?

The Director tasked me with four things:

1. **Increase the effectiveness of communication between the field and the headquarters' staff.**
2. **Standardize operations across the regions and missions. For instance, a facility clearance in one region should be the same as in another, especially for our larger companies with multiple facilities. That can also be related to reporting from the field.**
3. **Increase the responsibility of the enabling offices to support the field – IT, logistics, security, human resources, etc.**
4. **Increase the integration in the field across the mission areas.**

I think the first three are happening to some extent already, but no single person is driving the requirements or the changes. For the final one, the key is the regional directors and getting the right people in those positions

Given the Director's direction to you, what are your priorities?

My first priority is to establish a common understanding of how the relationship between the field and headquarters will change with the new construct. This is going to take a lot of work. We need to establish a common operating picture, identify gaps and then codify processes and procedures to close them.

My second priority is to provide a phased timeline of actions that will delineate everything that will happen as we move forward. This includes relevant hires, moves that will accompany that, and when to include shifting funding. We need to have clarity and transparency.

My third priority is to fill the new regional director positions. We've hired our first three, and I could not be more pleased. They are the right leaders for these critical positions.

You have been traveling a lot since you took this job. What have you learned? Did anything surprise you?

There have been a lot of surprises. I thought I had a pretty good understanding of what was going on in the field, but there is so much I didn't know. Many of our Background Investigation (BI) field offices who don't have NIPR capability, they are using wi-fi to log onto the network. There is a great disparity of support staff across the Regional Mission Directors (RMD). Maybe it's appropriate, maybe we need to make some adjustments.

And while I understood the talent and dedication of those working in the Field, I was impressed at how they are already leaning into mission integration. There are pockets of employees in every region working integration on an ad hoc basis. My job will be to provide the support necessary to keep those initiatives moving forward.

What challenges do you see?

The first challenge will be to relearn how to get things done. Who reports to who, how we effectively integrate — meat and potatoes staffing. Once we have successfully established the fundamentals, we need to get after integration and enabling support. If we move the ball forward in those areas, we're on the right track.

We hear 'integration' used a lot. How do you define it?

There are a lot of people trying to be too precise in how we define integration. We are going to figure out how to more effectively work together to support DCSA's mission. There are real obstacles: policies, authorities, etc. But there are also some obstacles that are framed by paradigms that no longer apply. There is information we can share that we are not. We can get better by simply understanding other missions within DCSA. As an example, Counterintelligence and Threat produces the MCMO [Methods of Contact/Methods of Operation] report. It contains valuable information about how our adversaries are seeking to exploit industry. The information in this report is invaluable to our background investigators working in industry, but many of the BI field staff had never heard of it. There are many similar instances where we have capabilities and resources that we are not sharing and its gaps like these that our enemies look to exploit

The agency recently announced the new regional directors. What skills did you look for in making these hires?

I wasn't looking for a subject matter expert in a particular mission area. They clearly need to understand the agency's missions and how DCSA fits into DOD and the security enterprise, but I was really looking for leaders who could help build a team and lead a team. I was also looking for leaders who could work together as a team. I wanted leaders, but leaders who would complement each other. That's the mindset I want in the field. Finally. I was looking for some fire in the belly. I believe this is an exciting time for DCSA — an incredible opportunity. I wanted to ensure they had that same passion for the mission.

DCSA employees part of DOD CIO award winning team

(From left to right) General Paul Nakasone, U.S. Cyber Command/ National Security Agency commander; Felicia Barbera, DCSA Counterintelligence Cyber Mission Center (CI-CMC); Chiedu Udebibe, CI-CMC; John Repici, Defense Cyber Crime Center (DC3); Joshua Black, DC3; and The Honorable John Sherman, Department of Defense Chief Information Officer, at the 2022 DOD Chief Information Officer Annual Awards for Cyber and IT Excellence ceremony on Dec. 9 at the Pentagon.

An example of DCSA's focus on this critical mission area is a recent collaboration with the Defense Cyber Crime Center (DC3) on a 12-month Defense Industrial Base Vulnerability Disclosure Pilot (DIB-VDP). The collaboration resulted in two DCSA Cyber Mission Center (CMC) employees being recognized as part of a DC3-DCSA team awarded the 2022 DOD Chief Information Officer Annual Awards for Cyber and IT Excellence. The DCSA CMC employees recognized for their efforts were Ashley Smith and Chiedu Udedibie, liaison to the DC3.

Planning for the DIB-VDP started in 2019, after DC3 and DCSA signed a Memorandum of Agreement and worked to identify mutually beneficial opportunities to pursue. DC3 already had an established VDP for DOD networks, and as part of the MOA, the agencies teamed on a 9-month research project culminating in a feasibility report exploring if the VDP could work for industry. The DIB-VDP would help industry secure its networks, and reduce supply chain risks and adversary attacks by minimizing the available attack surface. "Many large companies have a VDP in place, but the vast majority of cleared industry who handle controlled unclassified information can't afford to do this for themselves or have third party vendors do it," Smith said. "The thought was to see if DCSA could make it work for cleared industry."

After determining it was feasible, the DC3-DCSA team set forth to conduct a yearlong pilot focused on 10 small to medium sized companies. "We realized that 10 companies wouldn't be enough to keep the researchers busy, so we worked to enroll 41 companies total," said Smith.

A VDP is a process by which "white hat" ethical hackers report security flaws in an organization's internet-facing applications. During the pilot, white hat hackers explored the company's internet sites to uncover weaknesses, vulnerabilities, and misconfigurations that leave cleared industry assets open to adversary attack, supply chain risks, and exfiltration of DOD intellectual property. They then submitted reports via a platform that prioritized vulnerabilities by severity and tracked the mitigation progress. During the DIB-VDP pilot, the team processed over 1,000 vulnerability reports on small to medium participant DIB companies.

For the duration of the DIB-VDP pilot, the DCSA employees handled various aspects of the agency's responsibilities related to the initiative. Smith served as a program manager, worked the financing portion and helped recruit companies to participate in the pilot. Udedibie served as the onsite DCSA representative for the DIB-VDP pilot, keeping track of vulnerabilities, ensuring industry awareness and following up to determine if vulnerability mitigation techniques were successful.

During the DIB-VDP pilot, the team validated over 400 active vulnerabilities, 95% of which were successfully mitigated. This resulted in saving tax payers an estimated $61.6 million by discovering and remediating the active vulnerabilities on the DIB participant's public-facing assets, which if left unsecured would have brought severe damage to the DOD supply chain, DIB intellectual property, and controlled unclassified information. The partnership between DCSA and DC3 VDP allowed both agencies to use technical and strategic capabilities to support the effort and garner the most participation possible for the pilot.

"Based on feedback from the participating companies, the DIB-VDP pilot was a success and the companies were happy with it," said Smith. "This pilot widely limited the ability of our adversaries to walk into the networks of cleared contractors.

Leadership of PEO changes, part of continued agency transformation

As a part of the continued transformation of the agency, leadership of the Program Executive Office (PEO) transferred during a Change of Charter Ceremony on Nov. 15, 2022. DCSA Director William Lietzau presided over the event, accepting the charter from outgoing PEO Terry Carpenter and transferring it to incoming PEO Jeff Smith, who recently served as the Executive Program Manager of the National Background Investigation Services (NBIS).

In 2019, the deputy secretary of defense directed the transfer of several information technology acquisition programs to DCSA. The new mission required an acquisition capability to oversee the diverse IT development programs transitioning from across the federal government. The acquisition capability would need to achieve milestones and monitor costs to avoid volatile increases in budget requirements while delivering the best technology to help secure the U.S. government's technologies, services and supply chains. The entity was the PEO, formally established on Oct. 1, 2020.

"If you look at where we were a year or two ago, you will see how dependent we've been on PEO," said Lietzau while crediting Carpenter's leadership in building a program executive office that enabled DCSA to function as an agency. "We're now moving Terry to another part of the agency where we need him to start thinking about the future."

DCSA Director William K. Lietzau (left) accepts the charter from outgoing Program Executive Officer Terry Carpenter during a Change of Charter ceremony on Nov. 15 at the Russell-Knox Building. (DOD photos by Christopher P. Gillis, OCCA)

As the DCSA chief technology officer (CTO), Carpenter is charged with looking to the future to focus on long-term goals in developing the agency's information technology strategy.

In a workforce message, Lietzau explained the CTO role, "To oversee our research and innovation efforts and to develop a future-oriented technology strategy for the enterprise. This change consolidates several roles and activities presently in the Office of the Chief Information Officer (OCIO), PEO, and Chief Strategy Office. These changes reflect the natural maturation of the agency — the CTO leads our thinking regarding new capabilities for the future. After deciding on which capabilities the agency will invest, the PEO builds those capabilities and the OCIO ensures that the agency's IT systems support our mission on a daily basis."

> If you look at where we were a year or two ago, you will see how dependent we've been on PEO
>
> ***DCSA Director William Lietzau***

Carpenter received a DCSA Distinguished Service Award for his efforts as the PEO and was commended for his work on NBIS. Per the award citation: "Mr. Carpenter served with distinction leading the National Background Investigation Services program and the Program Executive Office. The security and testing foundations he put in place for NBIS were lauded throughout the Department as the model for large-scale agile software factory acquisition programs. Mr. Carpenter directed multiple initiatives that helped define and implement critical underpinning capabilities to support DCSA's digital transformation."

"It's enormous to think about what we've done with this ability to make our agency operate more efficiently. It's impossible to name everyone, but you trusted me, wrestled with ideas, you planted the seed and made them grow," said Carpenter. "I'm grateful for the opportunity to work with you and make a difference in national security."

As NBIS executive program manager, Smith managed the federal government's integrated information technology system for comprehensive personnel vetting — from initiation and application to background investigation, adjudication and continuous vetting.

NBIS is the federal government's one-stop-shop information technology system for end-to-end personnel vetting — from initiation and application to background investigation, adjudication, and continuous vetting. NBIS is one consolidated system designed to deliver robust data protection, enhance customer experience, and better integrate data across the enterprise.

DCSA Director William K. Lietzau (right) passes the charter to incoming PEO Jeff Smith, who recently served as the Executive Program Manager of the National Background Investigation Services (NBIS), on Nov. 15.

"I say it a little differently — we are not planting seeds but building a foundation. Each and every day, lay the foundation because you can't build a house without the foundation," Smith said. "Something we didn't talk a lot about — we were a PEO and we were NBIS, trying to fight two different battles. As of today, I get the opportunity to reconstitute PEO and make it one team, one fight. It is predicated in starting with a foundation. Agilely, this team will come together and add the building blocks to form a high performing PEO. I look forward to taking on that challenge."

Agency leadership works to forge one cohesive agency culture

By Daniel J. Lecce
DCSA Deputy Director

When DCSA was created in 2019, the agency combined numerous organizations into one. Each legacy organization brought their own distinct culture informed by proud histories supporting United States national security. Now, DCSA is building upon the strength of its legacy cultures to forge one cohesive agency culture that brings together the best of our collective talents and commitment to serve our nation.

"We must think differently than we have in the past about how our adversary is impacting us. We are being attacked on both the virtual and physical fronts. The fight has gotten complex. The role we play in securing the trustworthiness of the United States Government's workforce and protecting our nation's critical assets is indispensible to this fight. We, as Gatekeepers, are coming together as one unit with a unified culture, to better manage the threats as they come at us."

DCSA Deputy Director Daniel Lecce speaks during a Unity of Effort Road Show event in the Russell-Knox Building.

Establishing and maintaining a strong, common DCSA culture is paramount to preserving the Gate — protecting our nation's most sensitive information. The Unity of Effort goal in the DCSA Strategic Plan endeavors to unify efforts across mission areas by building a shared agency culture focused on public service and our nation's security. DCSA must transition from a collection of disparate missions operating in silos to an integrated security mission, working collectively as a single agency. An "enterprise mindset" will make the agency more effective, protecting the integrity of the nation's cleared workforce and technologies.

Rapid advances in technology, and a blended approach from our adversaries in nearly every domain, yield a more complex and dynamic threat environment than ever before. China's growing global influence and continued quest for domination in critical technology sectors increasingly threatens the American way of life. DCSA is the Gate and must meet the adversaries in kind with an integrated defense against all attacks, including the distinct threats China poses. As part of the Unity of Effort goal, leadership and the workforce must work together to establish a unified, inclusive Gatekeeper culture to reinforce commitment to this mission.

DCSA is cementing what it means to be a Gatekeeper. A Gatekeeper supports and defends against all enemies — foreign and domestic. Gatekeepers lift and lower the gate to our nation's entry point of information. Gatekeepers are mission-driven and essential to the security of our nation. The Gatekeepers of DCSA more effectively mitigate threats and drive positive mission outcomes when they adopt one agency ethos — one unified culture.

To continue building the Gatekeeper culture, we established the Unity of Effort Road show — a unique opportunity for me to engage directly with the workforce and hear their concerns. Building the Gatekeeper culture begins with leadership, and continues as a collaborative partnership among everyone in DCSA. For that reason, I traveled the country to:

- Communicate what it means to be a Gatekeeper in an evolving and increasingly challenging threat environment
- Gain workforce investment in helping to shape a culture of integration and Gatekeeper state of mind
- Drive unity of effort throughout DCSA and promote integration of DCSA's four distinct mission areas

Dr. Theresa Horne, director of the Office of Diversity and Equal Opportunity, briefs on the DEO Diversity, Equality, Inclusion and Accessibility plan during a Unity of Effort Road Show event in Fort Jackson, S.C. (DOD photos by Christopher P. Gillis, OCCA)

- Communicate the DCSA intent behind the Strategic Plan and the workforce's role and impact to success
- Collect input from the workforce to inform future projects to solidify DCSA as an employer of choice

Accompanying me was Dr. Theresa Horne, DCSA's Director of Diversity and Equal Opportunity (DEO). Supporting staff included the Deputy Director's Executive Officer as well as representatives from the Chief Strategy Office, the Human Capital Management Office, and the Employee Council (EC). EC representatives attended to represent staff across each organization/mission and relay pertinent information to the workforce they represent as well as agency leadership.

DEO's Diversity, Equality, Inclusion, and Accessibility plan is intrinsically linked to the DCSA Strategic Plan.

DEO Goals:

- Demonstrate leadership commitment and accountability to diversity, equity, inclusion, and accessibility efforts and promote sustainability

Alex Rivera, Human Capital Management Office, answers a question during a Unity of Effort Road Show event in Fort Jackson, S.C.

- Recruit, engage, and retain a diverse talent pipeline
- Ensure equity is at the center of an inclusive culture
- Leverage consistent, easily accessible programs for the diverse needs and abilities of the workforce

The Road show kicked off in Linthicum, Md., on October 19, 2022 and continued across the National Capital Region, then nationwide to DCSA field offices. Each Road show stop included activities designed for constructive conversations and collaboration such as All Hands focused on DCSA's Strategic Plan, America's biggest threats, and what it means to be a Gatekeeper. Dr. Horne followed by engaging the workforce on implementation of the DEO program. Then, leadership organized small focus groups of up to 15-20 people where we had candid conversations with the workforce about their DCSA experience. The constructive conversations from Road show stops will pave the way for a strengthened Gatekeeper workforce.

The Unity of Effort Road show signified more than just an opportunity for leadership and the workforce to engage. Lack of unity of effort could hinder our ability to secure the nation against serious and evolving threats; it is critical to maintain unity of effort in everything we do, from the Front Office to the Field. Accordingly, leadership will utilize Road show sentiments to identify short- and long-term actions to mold the Gatekeeper state of mind and solidify DCSA as an employer of choice.

DCSA's five-year strategic plan identifies nine goals that collectively help the agency achieve its mission and vision. Activity across DCSA's four mission goals (Industrial Security; Personnel Security; Counterintelligence and Insider Threat; and Security Training) and five enterprise goals (Talent; Unity of Effort; Operational Effectiveness; Digital Ecosystem; and Resourcing Processes) continues to ramp up in support of the plan. A cross-cutting key to the plan's success is the Unity of Effort strategic goal, which endeavors to "unify efforts across missions within DCSA through building a shared culture internally and engaging externally." Please reference Gatekeeper Volume 2, Issue 2's DCSA Strategic Plan 2022-2027 article for more information about strategic goals.

DCSA badges, credentials validate agency affiliation

By John Joyce
Office of Communications and Congressional Affairs

The record set by the Defense Counterintelligence and Security Agency (DCSA) Boyers Security Office verification team is official but you can't find it in the Guinness Book of World Records.

There is no competition world-wide regarding a verification team that confirms the identities of special agents performing official background investigator, industrial security and counterintelligence functions.

As the largest counterintelligence and security agency in the federal government, DCSA maintains a hotline and email address to verify the validity of badges and credentials that the agency's special agents and contract investigators present to those they are interviewing in the course of their investigative work to protect national security.

In turn, thousands of interviewees from security clearance applicants and their character references to security officers and small business owners in cleared industry will call that hotline or send an email to confirm the identity and authority of the special agent or contract investigator.

As fiscal year 2022 concluded, Matt Roman, chief of Security Operations for DCSA at Boyers, reflected on the number of times his team received a phone call or email requesting verification that a DCSA special agent or contract investigator's badge and credential are valid.

In all, Roman's four-member verification team fielded a staggering 21,504 requests from the public to confirm the identity of a special agent or contract investigator in every state of the union and overseas from Europe and the Middle East to South Korea and Japan.

The team's responses to the record setting number of verification requests comprised 12,622 phone calls and 8,882 emails throughout the fiscal year.

"Not one request for verification revealed a false badge or credential," said Roman. "We positively verified every badge and credential as valid since consolidating and transforming as one agency on Oct. 1, 2019. Although our team responds to a massive number of requests, the process is simple — we provide a name in response to the badge number or a badge number in response to the name of a special agent or contract investigator."

In previous years, the verification team — Shannon Bernard, Stacy Babcock, Stephanie Alvarado and Jon Hinkle — confirmed 16,156 verification requests in fiscal year 2021 and 19,428 requests to verify badges and credentials in fiscal year 2020.

"DCSA badges and credentials serve as validation for our industry partners and customers to confirm an individual is a direct representative of DCSA and acting in what capacity — background investigator, counterintelligence or industrial security," said Jason Benitez, senior program manager at the DCSA Security Office. "The purpose of the badges and credentials is to allow DCSA personnel the ability to conduct their daily operations by providing companies and customers the authorization, and affording customers the opportunity to validate the badges and credentials by calling the agency and confirming the individual is a DCSA representative. All badge and credential carriers must have at the very least a Secret clearance in order to conduct their daily responsibilities."

A senior advisor to the president's national security advisor observed the process Benitez described while at Boyers as the security team responded to verification inquiries, commending team members for their achievements during a visit in 2020.

"The Boyers DCSA Security Office is being recognized for providing exceptional customer service despite the limitations imposed by the HPCON-C [Health Protection Conditions – Charlie] measures," according to the justification for a DCSA award presented to Bernard, Babcock, Alvarado and Hinkle after the White House senior advisor recognized their "prompt, efficient service and professionalism in response to an investigator verification inquiry."

The award justification cited the team for ensuring there was no degradation of the verification or any of the primary services they provide during a 300% surge in verification inquiries from February to April of 2020.

"My team's verification of investigator identities coupled with our responses to complaints and requests for information is essentially a collateral duty," said Roman. "In addition to their primary security duties, the team also receives and processes returned badges and credentials while shipping and tracking badges expedited for mementos."

According to DCSA policy, badges and credentials are only issued to personnel in authorized credentialed positions — background investigators, industrial security representatives, counterintelligence special agents, contract background investigators, or contract investigative assistants.

"The verification is a reflection of the seriousness with which we want the public to take the badge and credential," said Jay Fraude, DCSA General Counsel. "We don't want anyone to have a fear or suspicion that someone who purports to work for us does not work for us. It's a privilege to be issued a badge. It is a mark of the great trust and regard, and high expectations of professional conduct, that we place in that person, especially since most of our folks, when they're out in public showing their badge to people, are not closely supervised. Their boss is not there."

DCSA Security issues three categories of credentials to the federal and contractor workforce as follows:

- Gold colored badge with credentials for federal civilian employees for identification in the course of their duties as background investigators, counterintelligence special agents and industrial security representatives.
- Silver colored badges with credentials for contract investigators and contract investigative assistants.
- Credentials for federal employees and contractor personnel who are not conducting investigations or assessments, but required for identification purposes in the course of duties such as records research and training.

Fraude cited published authority that has a bearing on why badges and credentials are issued and their effect.

The authority is a federal regulation – the National Industrial Security Program Operating Manual (NISPOM) Rule – promulgated at 32 Code of Federal Regulations (CFR) Part 117 on Feb. 24, 2021.

The NISPOM Rule, which applies to cleared contractor facilities, states the requirements for protecting classified information disclosed to or developed by contractors, licensees, grantees or certificate holders to prevent unauthorized disclosure.

In regards to credentials, NISPOM subsection 117.7 (f) – entitled 'Cooperation with Federal agencies' — requires contractors to "cooperate with federal agencies and their officially credentialed USG or contractor representatives during official reviews, investigations concerning the protection of classified information, or personnel security investigations of present or former employees and others (e.g., consultants or visitors)."

The NISPOM Rule then goes on to define that cooperation means as follows:

(1) Providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours; (2) Providing, when requested, relevant employment or personnel files, security records, supervisory files, records pertinent to insider threat (e.g., security, cybersecurity, and human resources) and any other records pertaining to an individual under investigation that are, in the possession or control of the contractor or the contractor's representatives or located in the contractor's offices; (3) Providing access to employment and security records that are located at an offsite location; and (4) Rendering other necessary assistance.

The effect to be given to official credentials during visits by U.S. government representatives is also covered in 32 CFR 117.16 (a) (3). This subsection – entitled 'Visits and Meetings' – states that "representatives of the USG, when acting in their official capacities as inspectors, investigators, or auditors, may visit a contractor's facility, provided these representatives present appropriate USG credentials upon arrival."

> DCSA badges and credentials serve as validation for our industry partners and customers to confirm an individual is a direct representative of DCSA and acting in what capacity – background investigator, counterintelligence or industrial security
>
> ***Jason Benitez***
> ***Senior program manager at the DCSA Security Office***

DCSA briefs industry on status of National Background Investigation Services development

By John Joyce
Office of Communications and Congressional Affairs

Jeff Smith encouraged cleared industry security officers to envision the National Background Investigation Services (NBIS) — a unified personnel vetting platform comprising background investigations, adjudications and continuous vetting — in terms of a house under construction.

The Defense Counterintelligence and Security Agency (DCSA) NBIS Executive Program Manager shared the analogy describing his NBIS vision to approximately 1,500 industry personnel security leaders and managers attending the 2022 NBIS Industry Conference in person and virtually to discuss industry's transition into the new personnel security vetting system.

DCSA Director William Lietzau provided opening remarks at the 2022 National Background Investigation Services (NBIS) Industry Conference on Oct. 18. (DOD photos by Christopher P. Gillis, OCCA)

"Iterative development of your house is no different than iterative development of this system," Smith said at the Oct. 18 event. "The first concrete, pillars and row of blocks are cross cutting investments that affect the rest of the house. So, if you're doing case initiations, adjudications or continuous vetting — this foundation has been built and laid as a cross cutting element."

The initial analysis based on traditional acquisition processes scheduled the complex information technology system for end-to-end personnel vetting to be ready for deployment in 2028. However, DCSA leaders — including the NBIS technical team and the agency's Adjudications, Continuous Vetting, and Background Investigation teams — would not accept that timeline, proposing a revised blueprint with an ambitious timeline to build the NBIS foundation collaboratively, innovatively and rapidly.

"We rebaselined that analysis to deliver NBIS in an optimum fashion," said DCSA Director William Lietzau in his welcoming remarks. "A new program with clear milestones was developed with a finish line to get us there and I can happily say that we're on a good trajectory with NBIS. The way we're building it is different from other DOD acquisitions. You've heard of Agile software — this is more than Agile software development. This is Agile programmatics, development and onboarding."

NBIS is built on Agile development principles that stress flexibility and incremental delivery of capability. It's designed with a single pane of glass concept that captures its configurability, scalability and cross cutting functionality to all users.

"This is also Agile deployment because we're actually using a system that hasn't been built yet," said Lietzau.

In addition to leveraging proven Agile techniques, NBIS is applying DevSecOps [stands for development, security and operations, which automates the integration of security into every step of development] pipeline approaches to software development. By facilitating fast, collaborative, incremental technology releases, these proven methodologies alleviate the need for broad system overhauls and will speed delivery, improve functionality, deliver customizable solutions, and enhance security. In this approach, NBIS users

will be able to provide feedback to inform requirement generation and lead to continuous implementation and improvement.

"NBIS is a holistic system for the U.S. government predicated on a very secure underpinning for cybersecurity," Smith said, adding that cleared industry is in the process of onboarding into the system with "highly configurable, scalable, multi-tenancy, cross-cutting and consolidated benefits."

DCSA is taking a measured and phased approach to move industry partners through a step-by-step process — reviewed thoroughly during the conference — to ensure a better user experience during onboarding.

Industry onboarding into NBIS is incremental and based on a facility's regional designation as identified in the National Industrial Security System. The incremental approach begins with DCSA's Western Region, then the agency's Eastern Region, Central Region, National Access Elsewhere Security Oversight Center and Headquarters and lastly, the Mid-Atlantic Region.

"NBIS empowers businesses while reducing the cost overall because it's a unified platform," Smith told the audience. "Our focus is improved interoperability and a holistic user experience because we're putting all our information in one frame of glass accessible by an adjudicator in our CAS [Consolidated Adjudicative Services], a continuous vetting analyst, or an industry partner as an FSO [facility security officer] submitting cases through the system."

At that point, Smith suggested that his audience of industrial security professionals are asking why they should care.

"The fact that we're putting everything on a single user interface — all data for the entire enterprise in an NBIS central repository," is a tremendous reason to care, said Smith while responding to his rhetorical question. "You're no longer on seven disparate systems. You never have to put information in this system and wait, wait, wait for business in the mission areas to move data through another system and give an answer or response. It's all happening inside one unified platform and that is huge — this has never been done."

The seven major systems being transformed on a unified platform founded on the underpinning of a robust cybersecurity foundation will ultimately create a seamless experience in the major mission sets — case initiation, continuous vetting, adjudications and background investigations.

Currently, case initiation — referred to as initiation, review and authorize functionality — is fully operational along with adjudications and various aspects of continuous vetting to support Trusted Workforce 1.5. The objective, according to Smith, is to have all legacy data migrated to NBIS, enabling organizations to perform subject management functionalities and expand DCSA CAS.

NBIS is the backbone of the Trusted Workforce 2.0 whole-of-government background investigation reform effort overhauling the personnel vetting process by creating one government-wide system that allows reciprocity across organizations. This includes the transition from periodic reinvestigations every five to 10 years to the Continuous Vetting Program, protecting the trusted workforce in real time. To reach that end state by Oct. 1, 2023, DCSA developed two transitional phases — Trusted Workforce 1.25 and Trusted Workforce 1.5.

"Often I hear," Smith said, "what's in it for me, what will it provide, and what's in it?"

In response to these questions, Smith said that DCSA is aware that corporate and small business facility and personnel security officers are certainly interested in case initiation and subject management.

"Today, you're going to hear a lot about it," he said in regard to case initiation. "They're (DCSA NBIS experts) about to bring you across the threshold. Some of you that are here today who will be on the panel later, have actually walked across that threshold. You'll talk about your experiences in the early stages. Actually, it was clunky maybe from your perspective as one of the early adopters from industry. That's fine

The former NBIS Executive Program Manager Jeff Smith gives an overview of the NBIS Program Status and emphasizes the value of Industry partnership.

and that's what we want to know. We're develop NBIS with the customer in mind with the influence of the customer in mind so that we get it right."

To ensure that DCSA and industry customers get it right, the remainder of the conference comprised DCSA briefings to industry security professionals on NBIS industry onboarding, NBIS capability and training for industry, NBIS Help Desk Support, and a panel discussion that included actions taken by NBIS resulting from industry feedback.

Scott DiStefano, NBIS division chief, provides a training product overview.

"Our personnel security mission improved in speed and quality," Lietzau said. "We could not do the continuous vetting we're doing right now if we did not put in place information technology that didn't exist (to create NBIS). There was some IT on the DOD side that allowed us to start cobbling things together. That's what got everyone in this room into a continuous vetting environment over the last couple of years. That's what drove our sequencing for NBIS. Now, the taxpayers are paying less because we've lowered prices three times and that's a good news story."

DCSA assumed operational control and responsibility for NBIS while it was still in development from the Defense Information Systems Agency on Oct. 1, 2020. The legacy background investigation information technology systems replaced by NBIS will be decommissioned in stages through 2023.

In all, NBIS will replace a suite of legacy background investigation and case management IT systems from the Office of Personnel Management and the Defense Manpower Data Center, including Electronic Questionnaires for Investigations Processing, known as e-QIP in addition to the Secure Web Fingerprint Transmission, Mirador, Defense Information System for Security, Position Designation Tool, Personnel Investigations Processing System, and more. With one consolidated system, security managers, investigators, and adjudicators can access case status throughout the lifecycle of a background investigation, enhancing capacity and creating synergies from easier data validation.

"We need you to partner with us to get NBIS off the ground and completely built much faster than it would have normally been possible using normal acquisition methodology," Lietzau told the industry audience, emphasizing that their feedback is crucial to perfecting the system moving forward as NBIS enables the Trusted Workforce transition from 1.5 to 2.0.

Multi-discipline DCSA team conducts facility review

Pictured in photo are (front from left to right) Randy Rosado, Aerojet Rocketdyne (AR); Billy Mitchell; Mark Lowery, AR; Chris Roesch, AR: Tammy Hendrickson, DCSA; Diane Horan, DCSA; Jessica Weedeman, DCSA; Katharine Kolwicz, DCSA; and Scott LaClair, AR. (Back from left to right) Stacy Wyatt, AR; Jonathan Stroud, AR; Doug Stone, DCSA; Rod Carter, AR; Robert Beecham, AR; Bailey Minard, DCSA; Wilkins Urquhart, DCSA; Mason Brauzer, DCSA; and Matt Knarr, DCSA.

In November 2022, members of the Industrial Security Herndon 2 Field Office, along with one team member from Herndon-1, formed a multi-discipline team to conduct a Security Review at Aerojet Rocketdyne Inc., in Culpepper, Va. The DCSA team included industrial security specialists, information system security professionals and counterintelligence special agents. The visit employed a new security review model that encompasses a whole-company approach and assesses security posture categories including 32 CFR, Part 117 "National Industrial Security Program Operating Manual (NISPOM) Rule" implementation, management support, security awareness, and security community. In preparation of the review, FBI in partnership with DCSA, provided the facility employees with an onsite threat briefing.

Aerojet Rocketdyne develops and manufactures advanced propulsion and energetics systems for customers including the U.S. Department of Defense, NASA and other agencies and companies, both in the United States and abroad. The company's markets include space, where they provide a full range of propulsion and power systems for launch vehicles, satellites and other space vehicles; strategic missiles; missile defense; and tactical systems and armaments. Aerojet Rocketdyne's propulsion systems, both liquid and solid-fueled, have been at the heart of virtually every major U.S. space and missile program since the dawn of the space age.

Security Professional Education Development (SPēD)

Program has six certifications, three credentials available

By Samantha Dambach and Jennifer May
Center for Development of Security Excellence

The Security Professional Education Development (SPēD) Certification Program is part of the Department of Defense's (DOD) initiative to professionalize the security workforce. This initiative is designed for individuals performing security functions on behalf of DOD and defines a common set of competencies. When security practitioners achieve these competencies, it promotes interoperability across DOD, facilitates their professional development and training, and creates a workforce of certified security professionals. The SPēD Certification Program is codified as a requirement for those individuals performing security functions on behalf of the Department in DOD Instruction 3305.13, "DOD Security Education, Training, and Certification" and DOD Manual 3305.13, "DOD Security Accreditation and Certification."

Since its inception in 2011, the SPēD Certification Program has delivered over 28,000 tests with an all-time pass rate of just over 51 percent. Currently there are over 10,300 active certifications and credentials with individuals employed at 48 different Federal agencies.

The program currently has six certifications and three credentials available. A certification is more general and broad in nature, and validates mastery across several knowledge areas, whereas a credential is more specific and intended for an isolated or specific audience. Credentials are stackable, which means they can be applied to or paired with an existing certification, and usually require less maintenance than a full certification.

Each certification or credential has its own set of eligibility and prerequisite requirements that candidates must meet prior to testing. For example, the Antiterrorism Credential is only for individuals currently serving in antiterrorism officer positions, while the Adjudicator Professional Certification (APC) and Due Process Adjudicator Professional Credential are only for individuals performing adjudication functions.

After meeting the eligibility and prerequisite requirements, candidates must attempt the test in a secure, proctored environment at one of the authorized testing centers. Candidates who pass the test and meet all other requirements are conferred for a period of two years. During that time period, individuals must obtain at least 100 Professional Development Units (PDUs), 50 of which must be security-related, to keep their certification or credential active. Various professional development activities, including completing training, attending conferences, or completing SPēD projects, are eligible for PDUs. Individuals who fail to obtain the required number of PDUs within two years will have their certification(s) or credential(s) expire.

Candidates who do not pass the test must wait at least 90 days before retesting (45 days in the case of the APC). This waiting period ensures candidates have enough time to prepare for their next attempt while also protecting the integrity of the test. Candidates have up to eight attempts per certification or credential.

Interested in learning more about SPēD certifications or credentials? Visit the Center for Development of Security Excellence (CDSE) website at www.cdse.edu/certification, or send an email to: dcsa.spedcert@mail.mil.

Core certifications:

- Security Fundamentals Professional Certification (SFPC)
- Security Asset Protection Professional Certification (SAPPC)
- Security Program Integration Professional Certification (SPIPC)

Specialty Certifications:

- Industrial Security Oversight Certification (ISOC)
- Physical Security Certification (PSC)
- Adjudicator Professional Certification (APC)

Credentials:

- Special Program Security Credential (SPSC)
- Due Process Adjudicator Professional Credential (DPAPC)
- Antiterrorism Credential (ATC)

Military Reservists on active duty assignments positively impact DCSA mission

By John Joyce
Office of Communications and Congressional Affairs

Did you know that DCSA — a DOD agency comprising more than 8,000 government civilians and defense contractors — is supported by military reservists on active duty who have joined their active duty Air Force counterparts to make an impact across the agency?

Who are the reservists, where and how are they supporting the agency, and what are their perspectives about DCSA's mission and impact on national security?

First, let's get to know them by name, military rank, DCSA title and the offices they support.

The current military team at DCSA includes the following reservists on active duty: Army Lt. Col. Jason Miller, senior contract specialist at the Office of Acquisition and Contracting; Army Maj. Remilekun Bankole, senior contract specialist at the Program Executive Office; Army Maj. Chris McLean, Reserve Integration Office (RIO) officer-in-charge; Virginia Army National Guard Capt. Nicholas Rivera, a 508 compliance officer at the Diversity and Equal Opportunity Office; Army Master Sgt. Vida Kwarteng, non-commissioned officer-in-charge and executive assistant at the Background Investigations Directorate; Army Sgt. 1st Class Travis Kelly, RIO non-commissioned officer-in-charge; Army Sgt. 1st Class Jennifer Valega, an analyst at the Counterintelligence and Insider Threat Directorate's Counterespionage Branch; and Air Force Staff Sgt. Clement Addo, a cyber-specialist at the Office of the Chief Information Officer.

Now, let's find out about their reserve support to the agency along with some of their perceptions and points of view that have developed since starting on active duty at DCSA, bearing in mind that some reservists are fairly new to the agency while others are well into their three-year tours.

"We are able to improve the DCSA mission by finding solid military personnel for numerous mission areas," said McLean. "These service members often bring substantial civilian-world experience and at a lower cost than government or contractor choices.

McLean and Kelly's RIO mission to facilitate reserve support requires coordination with agency leaders and the military services to develop full-time orders approved for reservists to support DCSA requirements. At that point, they advertise and find reservists who are interested and motivated to do so. Moreover, their coordination to integrate military reserve and National Guard support in the agency includes reserve drills — often two day stints — as well as annual training orders which normally run from two to three week assignments.

"Being at the foundational level means that we can ensure that the DCSA military force is relevant and impactful," said McLean. "We ensure that reservists can bring agency knowledge back to their units and that DCSA can learn from a variety of other agency and military experiences. This has been the best job that I have had – one in which I get to build something not only lasting, but that can pivot with new program experiences."

The reservists who volunteered for DCSA orders coordinated by McLean and Kelly reflected on the impact they are having on DCSA and how the agency impacts their careers.

"It's exciting being part of building a newer agency," said Miller, an acquisition and business advisor who develops acquisition strategies at DCSA to provide customers contract solutions tailored to their requirement and funding in accordance with the federal acquisition regulation.

"My experience in Army program offices and writing requirements for an Army signal command allows me to understand and relate to our customers," said Miller, in his second month at DCSA. "These orders are an excellent opportunity to broaden my professional experiences that

> We are able to improve the DCSA mission by finding solid military personnel for numerous mission areas
>
> ***Army Maj. Chris McLean, Reserve Integration Office (RIO)***

will add to the skill set for my civilian position with the Army."

"As a warfighter, my first and foremost responsibility is to serve and protect, which is in line with DCSA's mission considering the footprint we cover as an agency," said Bankole, who coordinates activities for the DCSA program executive officer while supporting the chief of staff's strategic vision for the agency. "Guided by the U.S. Army values, I am aligned with the unwavering integrity and passion DCSA gives to the American people. DCSA is open to new ideas and it's great to see that my perspective, background and experiences are welcomed to strengthen diversity, which births great ideas with no boundaries. This cultural innovation influences a high level of willingness and ability to be more agile in problem-solving and providing results."

Bankole is supports and assists with management cost, schedule, design, development and testing at DCSA. His goal is to deliver innovative enterprise enabling services, operations and business information technology systems that efficiently fulfill DCSA's mission.

"Working with DCSA is a high calling knowing how it affects the citizens of the United States of America," he said. "It is very rewarding to contribute to this cause and it will be an honor for any warfighter to join the team of the national gatekeepers who create security against foes who are foreign and domestic, thereby making the country safe."

Rivera, a former enlisted infantryman who became a military intelligence officer expert in personnel security, joined DCSA as a new addition to the Diversity and Equal Opportunity Directorate as the 508 compliance coordinator. Rivera — who deployed to Iraq and Kuwait and in his civilian capacity, served as a Norfolk, Va., police officer — is focused on creating a foundation for accessibility and inclusion for persons with disabilities to eliminate barriers in information and communication technology.

"I ensure that all administrative actions, as well as taskers, are complete and all products are presented at the highest standards on behalf of the Background Investigations (BI) Directorate," said Kwarteng, who serves as executive assistant to the BI director in support of the BI Executive Secretary Team's administrative functions.

"I've learned to take a different approach in requesting information or input," Kwarteng recounted. "The military approach is extremely direct and that can be taken a different way in a more civilian-lead organization. My DCSA tour of duty has certainly helped in expanding my range of professionalism. This opportunity allowed me to see another area of contributions toward defense that I was completely unaware of, and how it directly impacts our national security.

"I'm impacting DCSA network operations by managing real time network security solutions while making decisions on projects that affect the daily operation of DCSA," said Addo, a cybersecurity specialist who sets up new background investigation sites; works on network devices; monitors network outages; manages network projects; secures DCSA network devices and manages projects.

"While performing my duties at the agency, I've been enlightened on how to continue paying attention to details on simple information that is taken for granted," said Addo. "I'm learning more on how to manage people and projects' processes."

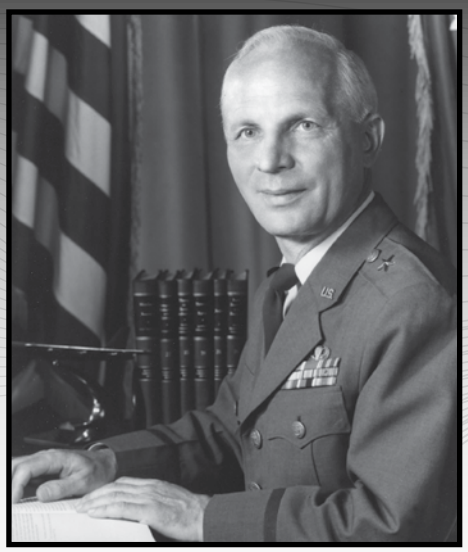
Building the Reserve Integration Office for DCSA is a once in a career opportunity," said Kelly, RIO senior enlisted advisor, who supports DCSA by leveraging military reserve and national guard talent during drill, annual training and full time orders. "I am honored to be part of something that will long outlast my time in uniform."

Kelly served in Korea and Fort Bliss, Texas, as a senior intelligence analyst and security manager. While in the Army Reserve, he was a chemical, biological, radiological and nuclear specialist instructor and a career counselor. As a civilian, he held several positions supporting the personnel vetting mission, including a DCSA position as a Federal Background Investigator Training Program instructor.

"The opportunity to use all the skills acquired from both my reserve training and civilian experience to better serve our nation has been not only rewarding but vital," said Valega, recently assigned as a special agent to the Counterespionage Branch. "As a reservist on active duty at DCSA, you get to be a part of the mission to safeguard the U.S., its workforce and trusted civilians from our nation's adversaries and their attempts to compromise sensitive national security information and technologies. DCSA truly is an agency with purpose and a place where you can learn from your supervisors and peers alike, which is something individuals in this profession should always seek out."

Valega is responsible for providing counterespionage and counterintelligence functional services to the national DCSA enterprise. She conducts an array of counterintelligence services, to include pre-briefs and debriefings for foreign travel; incident assessment activities; awareness and reporting; and collection in order to deter, identify, disrupt, exploit and neutralize foreign intelligence entities attempting to conduct intelligence activities against DCSA information, operations, facilities, systems and personnel.

Air Force career of first DIS director rich with intelligence, counterintelligence assignments



If you've been to the DCSA headquarters in Virginia, you may have seen the command wall in the Director's Suite. The only black and white photo is that of Air Force Brig. Gen. Joseph J. Cappucci. Before he was the first director of the Defense Investigative Service (DIS), he had a long military career and served in various assignments related to intelligence and counterintelligence.

After graduating from the University of Wyoming, Cappucci entered the Army Air Corps Reserve as a second lieutenant. He entered active duty in October 1940, and after completing Command and General Staff School, he was transferred to the European Theater of Operations.

His return to the United States in 1944 had him performing duties as a counterintelligence and intelligence officer in the Army Air Corps. He was detached to the Central Intelligence Agency in July 1946, followed by assignments in the Air Force Directorate of Intelligence, the Counterintelligence Division, and the Office of Special Investigations (OSI) upon its activation in August 1948.

He returned to Europe and held several counterintelligence positions before transferring to Offutt Air Force Base, Neb., to be the commander, OSI District 13. He held this position until February 1961, when he became the director of special investigations, Pacific Air Forces. In January 1964, he served in the Directorate of Special Investigations, first as the deputy director and later as the director.

In December 1971, the Air Force Office of Special Investigations (AFOSI) was created as a separate operating entity, and Cappucci retained his position as director of special investigations while also becoming commander, AFOSI. In April 1972, Cappucci was appointed the director of DIS, Office of the Secretary of Defense.

Much like other agency directors over the years, Cappucci was called upon to testify before Congress on the agency's operations and budget. In October 1973, he went before the House Appropriations Committee to advocate for approximately $22 million for fiscal year 1974.

"The DIS has been designed with the objectives of achieving monetary savings through eliminating duplications, of increasing managerial effectiveness, and of providing efficient and timely response to overall defense needs for personnel security investigations," Cappucci said in his opening remarks. "Those have been realized, as we have identified personnel savings of 12 percent, a 14-percent reduction in vehicles and attendants costs, and a 41-percent reduction in operating locations."

Cappucci clarified by noting that prior to the establishment of DIS, the three military services were operating at 417 locations, while DIS only used 246 — a reduction of 171 locations. Additionally, DIS had 416 fewer people and 243 fewer automobiles, "while doing the same amount of work," he said.

During his testimony, Cappucci had to justify his budget request for everything from personnel, to vehicles, a dedicated communications system, to teletypewriters.

"My agents drive the vehicles, and our vehicle fleet will travel about 16.3 million miles in fiscal year 1974," testified Cappucci. "When I got the automobiles from the three services, I got more than my fair share of old clunkers. So we plan to replace 293 sedans, because the cost of repairs is out of proportion to the value of the vehicle."

Additionally, the general was adamant during his testimony that DIS needed a separate, dedicated communications system to transmit information. "I don't feel that investigative information that consists of details of people's lives should go through communications that around the country," he said. "I think we have a responsibility here to protect reputations of people. Not only that, but to provide the necessary speed between my offices in the field to get the results in. This is also important because people cannot be put to work until they get a clearance. The sooner I can complete an investigation, the sooner they can be put to work."

Serving as the director of DIS was Cappucci's last assignment and he retired from the Air Force in 1974. As a civilian, he served as a security consultant. Cappucci died in 1992, and he and his wife Barbara are buried in Arlington National Cemetery.

Defense Counterintelligence and Security Agency

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