Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper

Volume 4, Issue 2

IN THIS ISSUE

IN THIS ISSUE

Vol 4 | ISSUE 2

DCSA Gatekeeper

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

FROM THE DIRECTOR

I am very pleased to have this opportunity to introduce myself to our readership and to share a bit of my early observations, our mission, and future.

As I read through the pages of this issue of The Gatekeeper, I was struck by the breadth of the agency's missions. I also was struck by how immediately relevant they are to our national security. So the results of our work really matter.

The threats we face are real. They are pervasive and relentless. There is war in Europe—the largest since World War II. We are also in a generational competition for advantage with China. Our adversaries and strategic challengers seek changes in the international rules based order that threaten democratic norms, our freedoms, and security. We see these challenges and threats abroad and domestically.

DCSA, our partners, and customers are on the front lines of this fight. We are a key part of the nation's first line of defense. I want to be part of this important work—that is why I wanted this job so much.

We enable trust. Strong security—security for our people, facilities, and information—that's what sets a strong foundation for, and enables trust.

- Trust in our nation's federal and industrial workforce—that they can join and remain a part of it. DCSA is key to the fundamental transformation of the federal vetting process.
- Trust in our industrial base—enabling industry's delivery of uncompromised capabilities. Our access to and partnership with industry ensure the protection of critical national defense information we rely on to prevail on the battlefield now and in the future.

I can already see how your hard work supports the agency's success, and U.S. and allied national security. Please know I recognize that our partners and customers are also critical to our successes. Intelligence and security are "team sports"—and we're in this together.

Everyone's role matters. I will never lose sight of that.

We need to ensure we are fit for purpose for today and tomorrow, seize opportunities and mitigate risks, and deliver on our important mission.

Over the next few weeks, I'll meet with DCSA leaders, our valued partners and stakeholders and you, the Gatekeepers, to hear directly how we can best ensure that DCSA is a great place to work and an agency that meets its mission. Please say "hi" as I visit our work sites, partners, and customers—I really want to get to know you and your work.

This is an exciting time for DCSA and I am honored and really excited to have been selected to serve as your director.

David M. Cattler
Director,
Defense Counterintelligence and Security Agency

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.

Heather C. Green is the Principal Deputy Assistant Director for Adjudication and Vetting Services for DCSA

In this capacity, Green manages over 1,000 personnel security specialists and adjudicators upholding protection of the Nation's workforce security. Programs under this scope include the: oversight of National Industrial Security Program (NISP) personnel security program, implementation of Continuous Vetting (CV) Program, Expedited Screening Center (ESC) and Adjudication Services. Adjudications customer base includes all military service members, military applicants, civilian employees, and consultants affiliated with the Department of Defense (DOD), to include the staff of the United States Senate and House of Representatives, the Congressional Budget Office, the United States Capitol Police, selected judicial staff, DOD personnel at the White House, and contractor personnel under the NISP.

In January 2023, Green assumed the role of leading the DCSA's Consolidated Adjudication Services (CAS), formerly known as the Department of Defense Consolidated Adjudications Facility (DoD CAF). CAS is the sole authority that determines security clearance eligibility of non-Intelligence agency DoD personnel occupying sensitive positions and/or requiring access to classified material, including Sensitive Compartmented Information.

Green was appointed as the Director of the Vetting Risk Operations (VRO), formerly known as the Personnel Security Management Office for Industry (PSMO-I), in February 2016. VRO provides a full spectrum of risked based operations to identify and address personnel security risk. VRO continuously evaluates personnel to determine access to classified information, facilities and equities as well as share information to mitigate insider threat risk.

From January 2013-February 2016, she led a dedicated team of Field Office Chiefs, Industrial Security Representatives, and Information Systems Security Professionals providing industrial security oversight to over 5,000 cleared NISP contractor facilities while serving as the Capital Region Director. From August 2011 to January 2013, she served as the Quality Assurance Manager for Industrial Security Field Operations (ISFO), conducting oversight of quality, consistency and standardization within ISFO. She was the Industrial Security Maryland Field Office Chief (FOC) with Defense Security Service from January 2002 to August 2011, where she provided management oversight of all aspects of the Maryland Field Office. She began her career with the Defense Security Service (now DCSA) in 1997, as a Special Agent conducting background investigations prior to moving into the industrial security field.

QUESTIONS AND ANSWERS

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

We are in a truly transformative period and have made significant advances to reform the Department of Defense (DOD) and Federal enterprise personnel security program. As the Principal Deputy Assistant Director for Adjudication and Vetting Services (AVS), I implemented visionary new procedural enhancements to create robust, timely, and multifaceted personnel clearance processes that addressed emerging trusted workforce policy requirements.

My number one priority is taking care of the AVS workforce as they play a critical role to the personnel security mission and ultimately protecting national security. My leadership team and I applied keen observation, engagement with the workforce, critical thinking, and a future-focused mindset to implement multiple process improvements and improve organizational integration, morale, and effectiveness. I've worked to improve and increase leadership communication, visibility, and accessibility for the workforce and seized the opportunity to increase cross-integration opportunities within the PS directorate, team building events and working groups to motivate and encourage employee engagement within AVS.

Can you tell us a little bit about what AVS does?

The merger between Consolidated Adjudications Services (CAS) and Vetting Risk Operations (VRO) is a significant milestone in the transformation of the Federal Government's personnel vetting system. Fiscal Year (FY24) will be a foundational period for the merger as the focus will be unifying Adjudications and Continuous Vetting workforces into a cohesive organization oriented around Trusted Workforce 2.0 and moving towards fully transitioning into the Working Capital Fund.

Assistant Director of Personnel Security, Dr. Mark Livingston has described this merger as a game changer. The AVS mission transformation efforts reflect our continued progress as we move toward "ONE PS." Coming together in this way gives our workforce an advantage and opportunity to perform better than ever and help us deliver on our commitment to mission first, people always.

The VRO oversees personnel security within the National Industrial Security Program (NISP) by validating and submitting Personnel Security Investigations for Industry and making Interim eligibility determinations for Industry's access to classified information. VRO also operates the Continuous Vetting (CV) program for the DOD, NISP, and 42 Federal partners monitoring more than 3.6 million national security personnel across the DOD and Federal enterprise. Our Expedited Screening mission develops uniform standards and a centralized process for the screening and vetting of individuals, with foreign influence and foreign preference concerns to include international partners, seeking access to DOD systems, facilities, and information.

I think we understand the mission of the CAS, but what should we know about adjudications?

Adjudications is an organization of over 800 federal civilian employees and contractors dedicated to ensuring individuals working for DOD as applicants, civilians, military members, contractors, consultants or others with physical or logical access to facilities and/or information systems, consistently meet the personnel vetting standards established by law, regulation and policy. Adjudicators, in conjunction with CV analysts, background investigators, human resources professionals, security managers and other vetting entities act as the Department's gatekeepers to the programs, missions and activities of the DOD. Our adjudicative team is the best at doing this work, both as the biggest and as the most effective large-volume adjudicative entity in the Federal Government.

You've seen quite a bit of change in your time at DCSA. How does this latest merger of VRO and CAS compare?

The merger is building upon the successes of VRO and CAS commitment to support TW 2.0. This merger will redefine the Federal Government's personnel vetting system, establishing a more dynamic and responsive organization, better equipped to navigate the challenges of tomorrow in the changing security landscape.

Stronger together, using the "One PS mindset", AVS will integrate the capabilities and expertise of both legacy organizations to utilize personnel and resources more effectively. As AVS matures, the unified workforce will be introduced to and trained on innovative processes and technologies tailored to improve the efficiency and impact of their roles across PS, equipping them with the necessary tools and skills to protect national security against current and future threats.

You have been on the forefront of implementing Trusted Workforce, can you tell us, in laymen's terms, what that means for DCSA and how it's going? In particular, what efficiencies or enhanced effectiveness should the DCSA workforce and stakeholders expect to see from this merger?

Trusted Workforce means an evolution of terminology, enhanced products, services and information technologies. Within AVS it means capitalizing on new information system capabilities to continue the high-quality products and services our customers have come to rely upon. That may involve further alignment of organizational business functions as we structure administratively to maximize the capabilities of our larger, combined [CAS-VRO] mission.

AVS promises to deliver enhanced continuous vetting and adjudication service offerings, improved response times, and optimized case management for our customers. We are carefully managing the transition to ensure service continues without interruption to the workforce. We continue to emphasize that "throughout this transformational period, it's essential that we maintain our focus on supporting the mission by ensuring our customers and stakeholders have the necessary products and services to protect national security."

As a significant step toward realizing the vision of Trusted Workforce 2.0, this merger will follow a phased, outcome-based approach with priority lines of effort and associated initiatives. The foundational phase will span much of FY24 and involve integrating critical operations, removing process redundancies, aligning functions with policies, and enhancing collaborative knowledge sharing within the personnel security directorate.

What has been the biggest challenge? And what successes would you like to highlight?

While we continue to make strides in the right direction, the biggest challenge has been ensuring we have enhanced automation to support our transformation efforts.

AVS has had several successes to highlight:

Enrolling the vast DOD cleared population, the world's largest, into a compliant CV program provides both immediate and long-term benefits to national security and has directly led to early identification of potential insider threat indicators. Prior to the implementation of the CV capabilities, the DOD and Federal enterprise relied on time-based periodic reinvestigations at 10- and five-year intervals depending on the level of clearance to identify derogatory information and potential insider threats. From 2021 to 2024, the CV program identified over 250,000 unreported actionable alerts requiring further investigation, which resulted in the revocation of 850 personnel security clearances. The program also exponentially increased the number of early intervention opportunities for leaders to employ corrective action with employees whose clearances might otherwise be endangered.

The CV program provides distinct advantage by identifying potential issues of concern much sooner than traditional periodic reinvestigations: an average of six years and seven months sooner for the Secret eligible population and two years and five months sooner for the Top Secret population. Without the early intervention that CV provides, it is likely that many issues upon which alerts are received would evolve into far more serious behaviors or problems for the subjects.

In FY23, our adjudication services have produced 700,000 cases closed in an average of 16 days, four days sooner than the 20-day Intelligence Reform and Terrorism Prevention Act timeliness standard for initial investigations and maintained DOD clearance reciprocity timelines at one to two days.

While prompt adjudication of clearances is important, AVS's key efforts took the focus away from pure end-to-end process timeliness and leaned forward to implement a risk mitigation approach to determine if a person is suitable for Federal Government work. DCSA's results were recognized by the Program Management Office of the Performance Accountability Council for reducing the average time needed to approve an individual to come to work via preliminary determinations to support critical missions. In the first quarter of FY24, the AVS's focus and success in issuing over 19,000 industry contractor preliminary determinations to achieve faster onboarding was highlighted as a new effectiveness measure in the Trusted Workforce 2.0 Personnel Vetting Quarterly Progress Update publication posted on performance.gov.

These efforts improved U.S. Government mission readiness and directly supports the President's Management Agenda Vision to transform personnel vetting to better identify risks and support mission readiness and workforce mobility.

What other changes are coming to AVS?

AVS is committed to excelling in all future TW 2.0 initiatives to support our customers and stakeholders with quality and timely products and services.

The merger brings us one step closer to a "ONE PS" approach in securing a trustworthy government workforce faster, better, and stronger.

I am also pleased to announce recent selections of the AVS Deputy Assistant Directors, Chakeia Ragin and Ryan Dennis! They both have extensive experience in personnel security and have already been change leaders making significant impact on personnel security transformation efforts.

In Chak's and Ryan's new positions they will play pivotal leadership roles in our transformation as we continue to navigate the different phases of the AVS merger. I am excited about the opportunities ahead of us as we integrate, evolve, and grow. Process improvements, finding efficiencies and leveraging the talent and skillsets of our amazing workforce will be key.

New Director leads DCSA

David M. Cattler was sworn in as the new DCSA Director by the Acting Under Secretary of Defense for Intelligence and Security Milancy D. Harris in a short ceremony at the Pentagon, Washington, D.C., March 25, 2024.

As the DCSA Director, Mr. Cattler will oversee a mission that uniquely blends industrial security, counterintelligence support, personnel vetting, and security training to advance and preserve America's strategic edge. He leads the agency's strategic transformation and maturation, and a workforce of approximately 12,000 federal and contract support personnel worldwide.

He has significant experience as a strategic leader, enterprise mission manager, and advisor. He has international experience with the North Atlantic Treaty Organization (NATO), and extensive experience within the United States federal government, including at the White House, the Department of Defense, and within the Intelligence Community. He is a veteran of the U.S. Navy with service as a surface warfare officer and an intelligence officer.

He has earned academic degrees from the U.S. Naval Academy and Georgetown University. He also is a graduate of the National Intelligence University, the U.S. Naval War College, and was a senior fellow at the Massachusetts Institute of Technology. He is the recipient of numerous national, foreign, and military awards.

Agency transitions to DOD 8140, starts using Cyber Workforce Compliance Manager tool

By Roxanne Landreaux
Office of the Chief Information Officer

In February 2023, the Department of Defense implemented DOD 8140 that identifies responsibilities for employees of the DOD cyber workforce and establishes a program with standard qualification requirements. It replaces the DOD 8570 Manual and its implementation is a multi-year phased approach for agencies. Currently, the Defense Counterintelligence and Security Agency is one of a handful of DOD agencies fully compliant in the requirements outlined within the new standards. This is important as the ongoing Joint Force Headquarters-DOD Information Network inspections are currently rating to this standard.

The DOD 8140-Manual outlines workforce identification, tracking, qualification, and was built to unify cyber workforce standards, establish a common data model with the DoD Cyberspace Workforce Framework, establish a more targeted approach for holistic workforce management, and finally, establish a program with standard identification and qualification requirements for interoperability.

While the 8570 series focused on attaining prescribed certifications to attain cyber compliance, the 8140 series is designed with organizational flexibility in mind, ensuring individuals have both the knowledge and capability to perform their assigned cyber work roles. The directive applies to four occupational series that are coded as cyberspace occupations.

DOD 8140 qualifications consist of three criteria to satisfy requirements: Foundational, Residential, and Continuous Professional Development (CPD). Foundational Qualifications are the initial requirements an employee needs upon entry to a cyber work role. In addition to baseline Foundational qualifications, 8140 introduces Residential Qualifications which includes on-the-job training and environment specific requirements for certain operating systems that apply to civilian and military personnel. This demonstrates a user's ability to perform their role in the workforce without supervision. The CPD requires that individuals engage in a minimum of 20 hours per year of professional development activities to maintain and enhance competence. This may be achieved through a variety of relevant activities including training, webcasts, seminars, and workshops.

The Cyber Workforce Compliance Manager (CWCM) tool is DCSA's new system that tracks and acts as a force multiplier to ensure cyber compliance. DCSA personnel can now easily manage and monitor their status in real time, using the tool to upload pertinent documents to maintain their cyber compliance. The user interface varies depending on if the individual is a general user or in a management position. The login process is simple, utilizing a CAC for authentication which brings the user to their profile. The tool provides all users with a "to-do" list and a compliance status. Users can update their compliance records by simply uploading the required items (certifications, transcripts, waivers, etc.) and verifying that they have been approved on their profile.

The CWCM tool supports supervisors and managers with expanded features. In addition to having all the same features of general users, leadership now has access to a Leadership Dashboard that features enhanced reporting options. Managers will have access to graphs succinctly showing the compliance status of all groups assigned to them, along with custom reports which can be downloaded according to the desired parameters of the user. If a supervisor manages multiple groups, they can view the compliance of each group individually or assign an action officer to a group for task delegation. Overall, the CWCM tool is a one-stop shop for all cyber compliance needs required for DOD 8140.

New Program Executive Officer, NBIS program manager come on board at DCSA

The Defense Counterintelligence and Security Agency welcomed two senior leaders recently.

Robert "Rob" Schadey is the new Program Manager for the NBIS

Edward Lane joined the agency as the Program Executive Officer (PEO) on April 24. In this role, Lane is responsible for the direction and synchronization of multiple portfolios of information technology (IT) systems that support both federal and defense services for DCSA operations. The IT systems include the National Background Investigation Services (NBIS), National Industrial Security System and the DITMAC System of Systems. In this capacity, Lane will be responsible for the cost, schedule and performance of these IT systems.

Lane has a deep leadership and acquisitions background in both the private sector and government. He has prior military and government experience at the Office of the Under Secretary of Defense for Intelligence and Security and the National Reconnaissance Office. His last federal position was as the Deputy Senior Acquisition Executive at the Defense Intelligence Agency where he led all acquisition and contracting to execute over $15 billion and over 2,200 annual contract actions across the spectrum of products, supplies, facilities, services, and development programs in support of the Intelligence Community and Combatant Commands.

Robert "Rob" Schadey is the new Program Manager for the (NBIS), effective March 10. In this role, Schadey provides strategic planning and technical and analytical support related to acquisition, cost management, scheduling, development, and performance for the NBIS. He also develops NBIS policies, procedures, and strategies governing the planning and delivery of services throughout the organization and integrate NBIS programs and services.

NBIS is the federal government's information technology system for end-to-end personnel vetting — from initiation and application to background investigation, adjudication, and continuous vetting. NBIS will be one consolidated system designed to deliver robust data protection, enhance customer experience, and better integrate data across the enterprise. NBIS is the foundation for future technology and policy requirements. As the federal government looks to reform and modernize its personnel vetting processes with Trusted Workforce 2.0 policy changes, NBIS will play an integral part. The system will leverage technology to improve delivery and capabilities.

Prior to joining DCSA, Schadey served as the Acting Deputy Program Executive Office Enterprise Information Systems (PEO EIS) with the U.S. Army, where he led and advised on digital transformation, stakeholder engagement, agile delivery of solutions, as well as developed and recommended innovative approaches to manage and streamline programs and processes. While at EIS, he also served as the assistant program executive officer and was director of the Business Mission Area at PEO EIS. He was responsible for integrating and modernizing the Army's enterprise resource planning systems, focusing on enterprise initiatives such as cloud migration, cloud computing and data analytics.

Agency holds first National Industrial Security Program Signatory Workshop

By Dante Swift
Office of Communications and Congressional Affairs.

On Feb. 9, 2024, DCSA Industrial Security directorate hosted its first National Industrial Security Program (NISP) Signatory Workshop in the Russell-Knox Building. More than 80 government partners participated in the workshop in person and virtually.

The NISP was established by Executive Order 12829 to ensure that cleared U.S. defense industry safeguards the classified information in their possession while performing work on contracts, programs, bids or research and development efforts. DCSA administers the NISP on behalf of the Department of Defense and 35 other federal agencies. There are approximately 12,500 contractor facilities that are cleared for access to classified information under DCSA's security oversight responsibilities. DCSA provides field personnel, Government Contracting Activities (GCAs) and cleared contractors with timely, consistent policy guidance and effective interpretation of the NISP.

Assistant Director for Industrial Security (IS) Matthew Redding opened the workshop reflecting on the transformation of DCSA from the legacy Defense Security Service, and he shared his perspective regarding where the nation stands against its adversaries.

"It's important that the federal family, those who have signed on to the National Industrial Security Program, recognize that your job and your agency is the most important component because you oversee and administer classified contracts," Redding said. "Each one of your agencies has a national security role and that means defending the nation and overseeing compliance."

Redding continued his reflections, highlighting the accomplishments the industrial security team had made, to include transferring legacy functions to Field Operations, while concurrently preparing for the transition from the National Industrial Security System (NISS) to utilizing NISS Increment II (NI2) capabilities, acquisition and government strategy.

He closed out his comments by looking ahead, noting the directorate is progressing toward a number of goals such as enhancing field operations, formalizing the continuous entity vetting process and working on building up entity vetting capability.

Assistant Director for Industrial Security Matt Redding (left) provides opening remarks at the NISP Signatory Workshop on February 9 in the Russell-Knox Building, Quantico, Va. (DOD photo by Christopher P. Gillis)

Keith Minard, IS Policy, shared the latest policy updates relating to industrial security, to include the process for getting Industrial Security Letters (ISLs) released. ISLs are issued periodically to inform cleared contractors, GCAs and DOD entities of information and clarifications of existing policy and requirements relating to industrial security. Prior to the new process, ISLs needed to be approved by the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)). Now, ISLs are reviewed by the Office of Management and Budget to ensure that they meet requirements and can be issued as guidance and then are approved by the Director, DCSA for issuance.

"We have worked on a lot of things that are challenging to do our mission to ensure it is successful not only for you but also to enable the cleared contractors to fulfill their duties efficiently," Minard said.

In addition to Minard, Allyson Renzella, who serves as the IS branch chief in OUSD(I&S), provided information regarding updates pending to 32 CFR Part 117, "NISP Operating Manual (NISPOM) Rule."

"There are many factors at play, the most important being that it is an election year," said Renzella. "Rule making ceases because the federal government does not want to

place new rules into play with the potential of having a new administration gaining control and reversing the new rules that just passed."

Minard closed with, "DCSA works with the NISP community to enable you as signatories."

Kevin Williamson, senior action officer, NISP Mission Performance, emphasized that DCSA serves as the "front line trace of the field workforce", and briefed on the security rating process.

"The agency conducted 3,632 security reviews for fiscal year 2023 and 99% of the companies achieved a rating of at least satisfactory," he said, noting the ratings reflect the guidance provided by industrial security representatives and GCAs, as well as updates made to the security review process.

"We are committed to protecting your exterior companies, your assets and your people by educating, training and providing resources and support to confidently handle classified information," he said.

"We understand that while we are in an oversight element, our goal is that these companies are all compliant and continue to support the respective signatory on their classified programs," Williamson concluded.

The NISP Authorization Office (NAO) serves as ground zero for the monitoring of authorized information systems that process classified information as part of classified contracts.

"The NISP Authorization Office serves as the nexus between field operations, the Department of Defense and our government partners," said Jon Cofer, a designated representative within NAO. "In our execution of the risk management framework, we produce the external guidance that lets industry know how to configure and how to continuously monitor these information systems."

By using interconnection agreements, such as memorandums of understanding and memorandums of agreement, sometimes in conjunction with interconnection security agreements, DCSA provides oversight of contracts operated by cleared contractors who process classified information.

Jon Cofer, National Industrial Security Program Authorization Office in Industrial Security, discusses the agency's role in authorizing information systems that process classified information within cleared contractors during the NISP Signatory Workshop on February 9 in the Russell-Knox Building, Quantico, Va. (DOD photo by Christopher P. Gillis)

"An interconnection security agreement is a document that details the technical configuration of a connection," said Cofer. "It details how that connection is executed, how it is secured and the physical and logical administrative security controls that are applicable for that connection."

Cofer went on to discuss the importance of the Enterprise Mission Assurance Support Service (eMASS), which is the web-based application used for comprehensive fully integrated cybersecurity management. It provides an integrated suite of authorization capabilities and prevents cyber-attacks by establishing strict process control mechanisms for obtaining authorization decisions. This application is used to identify how many systems are currently registered within industrial security, placing the authorizations into six categories, such as authorization to operate, expired, to not yet authorized.

"The system itself is operating to standard as it is interconnected with our operations," said Cofer. "Our authorization timelines are getting better every day," noting that DCSA has 5,600 registered systems, 3,600 NISP eMASS users and 2,200 authorizations processed in Fiscal Year 2023.

The NISP Signatory Workshop is an example of the agency working to strengthen its partnerships through continuous cross-collaboration as it continues the mission of America's Gatekeeper.

Agency partners with industry, government stakeholders to refine security rating process

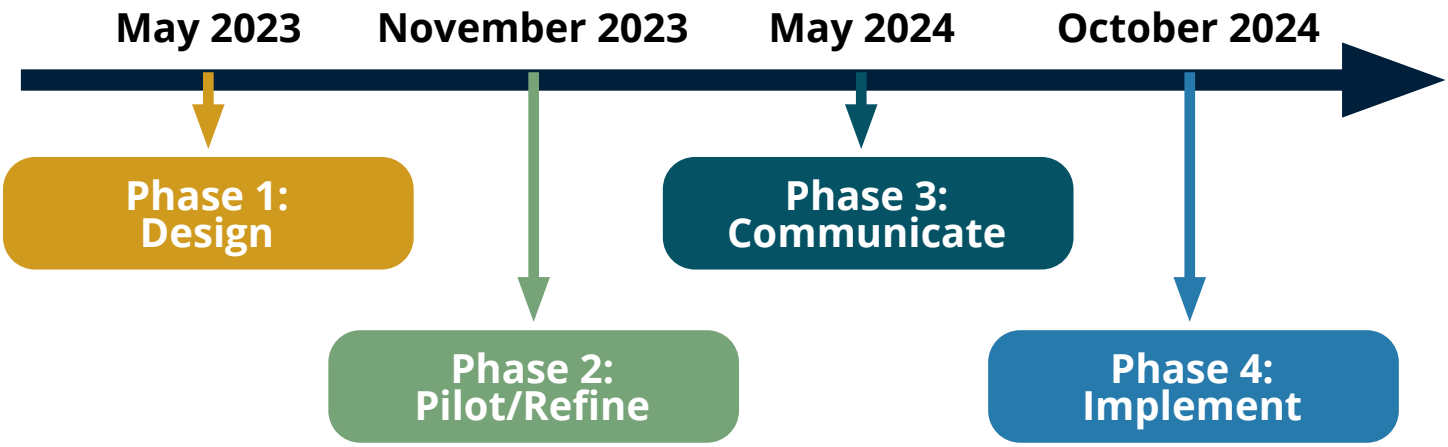
By Misty L. Crabtree
Industrial Security Directorate

As Henry Ford, an American industrialist and founder of the Ford Motor Company, once said, "be ready to revise any system, scrap any method, abandon any theory, if the success of the job requires it." In 2023, DCSA was ready to refine its security rating process, which had been fully implemented in September 2021.

This process, firmly anchored in DoD 5220.32 Volume 1 policy, is compliance-first, criteria-based, and uses a whole-of-company approach to calculate security ratings. Compliance-first meant eliminating the offsetting use of "enhancements." This means that DCSA no longer considers a contractor for a higher than satisfactory security rating if there are any critical vulnerabilities or serious vulnerabilities characterized as systemic. Again, compliance comes first! After two years using the security rating process, it worked as intended and the results aligned with historical norms. However, just because a process works, doesn't mean it can't be improved.

In collaboration with Industry partners and Government stakeholders, Industrial Security zeroed in on two key refinements: incorporating a numeric score and clarifying criteria requirements. In other words, coming to agreement on key definitions. The goal of the security rating refinements is to create and implement a fair and simple process that minimizes subjectivity and increases consistency, quality, and transparency. The refinements will not impact the current security review process in any way. In May 2023, DCSA began working on the security rating process refinements, known as the Security Rating Score (SRS) project. Internally, a field-centric and cross-regional working group was established to leverage subject matter expertise and drive design efforts. This working group kicked off in June 2023 and meets twice a week. Externally, in partnership with the National Industrial Security Program Policy Advisory Committee (NISPPAC), a NISPPAC Industry SRS Working Group was established to provide feedback on the design, highlight concerns, and consult on the pathway forward. This working group kicked off in August 2023 and meets every two weeks. Additionally, Industrial Security periodically briefs and obtains feedback from Government stakeholders.

The SRS project has four primary phases: Design, Pilot and Refine, Communicate, and Implement. The Design Phase concluded in November 2023 and resulted in criteria refinements and a finalized provisional security rating score model. The key to this design was the invaluable



partnership between DCSA, Industry, and Government stakeholders. The provisional design includes many highlights:

- Consolidates the two lists of criteria under the current security rating process into a single list of criteria known as the "gold standard," with additional guidance that further defines each criterion. This element addresses subjectivity and inconsistency concerns.
- Adds a numeric score component which decouples the final security rating from individual category ratings assigned under the current security rating process. This means the lowest category rating will no longer determine the final security rating nor will a contractor have to achieve 100% of criteria to obtain higher than a satisfactory rating. This element addresses fairness and simplicity.
- Provides granular feedback within the Security Review Rating Scorecard on which criteria was or was not achieved. This clearly documents facility successes and opportunities for growth and shows how DCSA calculated the security rating score. This element addresses transparency.

The SRS project is currently in the Pilot and Refine Phase, during which DCSA will use data collected as part of approximately 41 security reviews conducted during the second quarter of fiscal year 2024 to independently calculate a security rating score under the provisional design. The consolidated results and feedback will help DCSA and the NISPPAC Industry SRS Working Group validate if the numeric score design element works as expected and assess if additional refinements are needed prior to finalizing the model. Looking forward, if no major refinements are needed after the pilot, DCSA will begin executing a robust communication and training plan in May through June 2024 as part of the Communications Phase. The goal of this phase is to ensure all stakeholders understand the refinements and are prepared to fully implement on October 1, 2024.

In the words of Henry Ford, "coming together is a beginning, keeping together is progress, and working together is success." During the SRS project, the continued support of Industry partners and Government stakeholders, as well as the continued collaboration and buy-in are vital to improving the security rating process.

World War II slogan crucial to preventing unauthorized disclosures

DITMAC team working to reduce UDs, train DOD workforce

By John Joyce
Office of Communications and Congressional Affairs.

It was World War II and the "loose lips sink ships" slogan sprang up throughout the United States from billboards and posters to Hollywood productions advising Americans in the military, government, industry and the public to prevent inadvertent disclosure of important information to the enemy.

"It's just as true and crucial today as it was throughout World War II," said Andy Rovnak, DOD Unauthorized Disclosure Program Management Office (UDPMO) chief. Rovnak was reflecting on how the U.S. Office of War Information's campaign to protect critical information focused on specific rules of conduct established to protect strategic military plans, national security, the American people, and warfighters deployed on two fronts and around the globe.

"Deterring, detecting and mitigating unauthorized disclosure is everyone's responsibility—it's our military, government and civic duty," said Rovnak in a February 2024 interview with DCSA Gatekeeper magazine. "We've got to be very careful in what we say and do. We're not just talking on the phone, – we're on cyber while people are trying to compromise the integrity of our networks and our cyber capability. It's where we are right now in the state of the world, and we must avoid any release of classified or secure information which could damage our national security."

Rovnak leads the UDPMO team, – one of several DCSA counter insider threat teams comprising the DOD Insider Threat Management and Analysis Center (DITMAC), – in their efforts to help prevent unauthorized disclosure or leaks of non-public information, crucial to maintaining the nation's security, personnel safety and public trust.

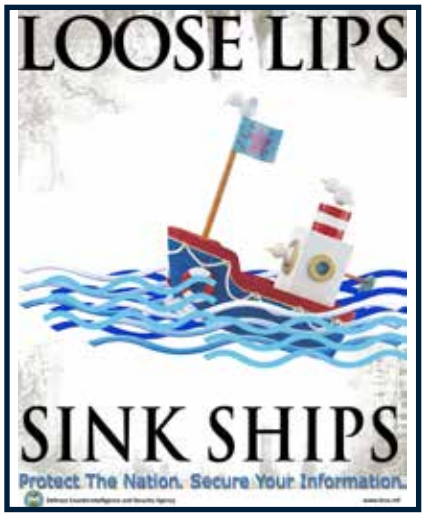
"The 'loose lips sink ships' campaign also applies to the unauthorized disclosure of sensitive unclassified information," he said. "Although unclassified, this sensitive material could enable our adversaries and any potential adversaries to identify and exploit vulnerabilities. It would allow them to steal and use our intellectual property and technology against us, leading to an increased risk of mission failure and potential loss of life."

An unauthorized disclosure occurs when trusted individuals inside an organization communicates or physically transfers classified national security information or controlled unclassified information (CUI) — including Operations Security critical information and indicators — to an unauthorized recipient.

Andy Rovnak
Chief, DOD Unauthorized Disclosure Program Management Office

"There are multiple threats out there and we're losing intellectual property to unauthorized recipients," said Rovnak, pointing out that recipients span external threats such as nation state actors to criminal entities who target the federal government, defense industrial base and American citizens. "If information in the care of government on behalf of its citizens to protect the nation is exposed, – someone will take advantage of it. The same is true with personal information. The technological revolution and transformation into a digital society since the World War II era resulted in a fragility in how we operate from an information standpoint that didn't exist back then. Someone without nation-state capabilities can interfere and cause a significant amount of damage. They're able to get the information quicker now and turn it around faster against us. If someone knows about a vulnerability, that person can use ChatGPT and write code that may go out to exploit that vulnerability."

This knowledge released through an unauthorized disclosure of classified information or CUI can happen in various ways. It could be disclosed intentionally, negligently or inadvertently through leaks, data spills, espionage and improper safeguarding of national security information. When classified information is involved, unauthorized disclosure can be categorized as a type of threat or security incident, characterized as an infraction or violation depending on the seriousness of the incident.



"My UDPMO team coordinates the reporting of unauthorized disclosures within the Department of Defense to ensure prompt and complete delivery of case referrals to the Department of Justice and DOD senior officials for administrative action, civil remedies or criminal prosecution," Rovnak explained. "We are also charged with promoting collaboration and information sharing of unauthorized disclosure information across DOD and the intelligence community."

Since April 2023 when he arrived at DCSA, Rovnak carried out his UDPMO vision to provide continuous workforce engagement activities that reinforce the importance of protecting DOD information from unauthorized access or disclosure while providing it to those who need it, plus gaining efficiencies to deter, detect and mitigate instances of unauthorized disclosure.

"This requires a deliberate enterprise-wide effort to ensure everyone understands the importance of appropriate information sharing and safeguarding across the department and the role they have in providing protection of classified national security Information and CUI from those who don't have an appropriate need to know," said Rovnak. "Our goal for this year is to provide a measurable reduction of DOD unauthorized disclosures through focused security awareness training activities that change human behavior toward the direction of prevention. We are planning to increase collaboration and engagement with the workforce as key elements to improve the identification, investigation, tracking and reporting of unauthorized disclosures in 2024."

The Unauthorized Disclosure of Classified Information and CUI course, available on the Center for Development of Security Excellence (CDSE) Security Awareness Hub, provides an overview of unauthorized disclosure, including specific types of unauthorized disclosure and some common misconceptions about unauthorized disclosure. The course also discusses the types of damage caused by unauthorized disclosure and the various sanctions one could face if caught engaging in unauthorized disclosure. CDSE also provides resources to bring security expertise straight to any organization, including those for unauthorized disclosure.

In support of the January 2024 OPSEC Awareness Month, the UDPMO held three 'Unauthorized Disclosure 101' briefs to the DOD workforce, attended by over 350 individuals.

The UDPMO team is immediately notified of all incidents involving the release of classified national security information and CUI in the public domain. Notifications to UDPMO include the release or enabled theft of information relating to any defense operation, system or technology determined to be classified national security information or CUI.

The team is also alerted to incidents of classified information or CUI disclosed to an unauthorized person or persons resulting in an individual's administrative action, referral for criminal or counterintelligence investigation, or the suspension or revocation of a security clearance.

"Everyone has a civic duty to say something if they see an unauthorized disclosure," said Rovnak. "If they report it to us, we can work to mitigate it, but I need to be informed. It's crucial to report a potential unauthorized disclosure to the appropriate authorities."

When UDPMO receives a confirmed report of unauthorized disclosure in the public domain, the team submits a crime report to the Department of Justice. Included in the report are findings from a preliminary inquiry conducted by the affected component; a damage and impact assessment; and a media leaks questionnaire for the unauthorized disclosures appearing in the media.

In terms of reporting unauthorized disclosures, the DOD Whistleblower Protection allows individuals to report information they reasonably believe provides evidence of a violation of any law, rule, or regulation, gross mismanagement, a gross waste of funds, abuse of authority, or a substantial danger to public health and safety to designated officials via specific channels.

Additional information regarding DoD Whistleblower Protection is available on the DoD Inspector General website at www.dodig.mil. Those making contractor disclosures in response to Federal Acquisition Regulation clause 52.203-13, Contractor Business Ethics Compliance Program and Disclosure Requirements, can find relevant instructions at www.dodig.mil/Programs/Contractor-Disclosure-Program. The differences between unauthorized disclosure and protected whistleblowing are further clarified at https://www.cdse.edu/Training/Toolkits/Unauthorized-Disclosure-Toolkit/.

Generative Artificial Intelligence could increase cyber threat to cleared industry

By Counterintelligence and Insider Threat Directorate Cyber Mission Center

Generative Artificial Intelligence (Gen AI) tools—like the commercially available OpenAI's ChatGPT, BingAI, or Google's Bard—are rapidly evolving and becoming more popular across the defense and private sectors. Many organizations in the private sector pilot innovative Gen AI projects aimed at incorporating these tools into their mission and business. Using learning algorithms, Gen AI tools summarize, predict, and generate convincing conversational texts, audios, images, videos, and/or other forms of media that mimics a human's timely response. Employees can use Gen AI tools to query massive datasets, automate security data, write simple and complex software programs to produce analytical and financial prediction models, identify and fix network vulnerabilities, and respond to cyber threats.

In a January 2024 Defense Scoop article, Defense Information Systems Agency (DISA) technical director Andres Malloy shared how the Cyber Development Directorate is exploring Gen AI tools as a force multiplier for the DOD in relation to cyber threats and the handling of different malware variants.

Malicious actors are employing Gen AI chatbot tools to conduct more effective, faster, and sophisticated cyber operations. First, they are exploiting the Gen AI craze by creating fake Gen AI service websites, which mimic legitimate sites and advertise fake Gen AI tools as a paid subscription. These websites put potential customers at risk of sharing financial information or downloading disguised AI-powered malware software. In addition to these websites, an overabundance of sophisticated copycat Gen AI chatbots are available on the Dark Web. These copycat tools assist malicious actors with writing undetectable AI-powered malicious malware and building sophisticated hacking tools. They use these hacking tools to quickly probe an organization's public facing network, identify unpatched vulnerabilities, and exploit these vulnerabilities for nefarious purposes.

Malicious actors are also employing Gen AI tools in targeted phishing campaigns. First, they scour organizations' websites to identify the company's executive officers, financial officers, and key personnel. Next, using sophisticated Gen AI tools, they quickly scan social media and other public platforms to collect the individuals' publicly available postings, images, and/or audios. Armed with this knowledge, Gen AI then lifts 2D images, turns them into 3D images, and produces manipulated media called Deepfakes. Finally, malicious actors employ these manipulated videos/audios to: (1) damage a company's reputation, value, and brand; (2) gain unfettered access to an organization's personnel data, its operations, and sensitive financial, proprietary, or internal security information; or (3) impersonate a company's customer base to gain access to customer accounts.

Deepfake media is likely becoming a major concern for the DoD. In a mid-2023 Defense Scoop article, National Security Agency cybersecurity director Rob Joyce stated, "Malicious foreign actors craft very believable native language, English text that could be part of a phishing campaign." Business email compromise schemes are the most common version of this threat. Using previous conversations between the vendors and their customers, the Gen AI tools replicate the conversation's language to target and convince a company to disburse funds to fraudulently controlled accounts or install malicious malware.

Foreign threat actors will likely employ Gen AI tools to conduct cyberespionage, steal intellectual property, gain financially, or spread false information in 2024. DCSA's Cyber Mission Center (CMC) is here to assist Cleared Industry with identifying and assessing potential cyber threats. Cleared Industrial partners can submit, at no cost, emails they suspect contain malicious attachments to DCSA's Joint Cyber Intelligence Tool Suite (JCITS) Malware Intelligence Triage Tool (JMITT) tool. JMITT is a platform designed to safely conduct analysis on the suspicious email for any potential threats, returning results within minutes to enable a timely, informed decision. The tool also identifies potential connections to nefarious cyber entities through identified indicators of compromises (IOCs). These IOCs are shared with other DCSA tools for additional analysis of trending cyber threat activities, tactics and techniques. Please contact your local Counterintelligence Special Agent for additional information on DCSA CMC capabilities and how the CMC can assist you further.

Agency exceeds its small business goals in several categories

By Office of Small Business Programs & Industry Engagements Team

For the second consecutive year, the Defense Counterintelligence and Security Agency exceeded its annual statutory Small Business Goals. Through the efforts of the Office of Small Business Programs and Industry Engagement (OSBP&IE), who works to maximize small business participation in support of a whole-of-enterprise approach in securing the trustworthiness of the U.S. Government's workforce and the Nation's critical assets, the agency exceeded its goal achievement numbers in various categories.

During fiscal year 2023, the agency awarded:

- Over $300 million to Small Businesses,
- Over $200 million was awarded to Small Disadvantaged Businesses,
- Over $25 million was awarded to Service-Disabled Veteran-Owned Small Businesses,
- $50 million was awarded to Women-Owned Small Businesses,
- $16 million was awarded to Historically Underutilized Business Zone.

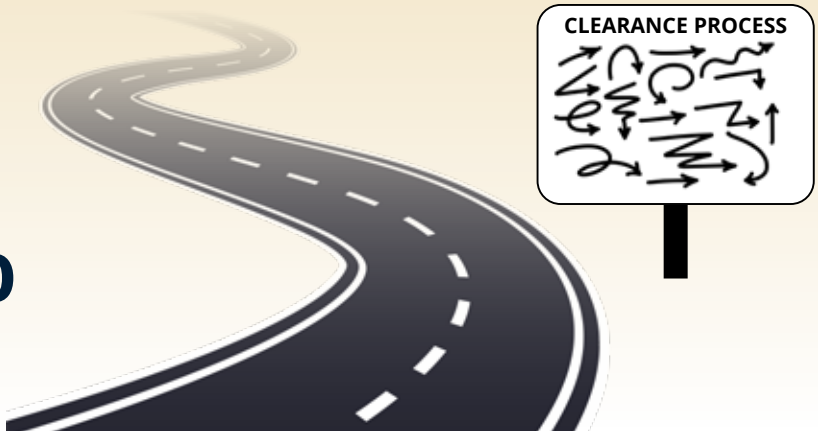
In its efforts to ensure the agency harnesses the power, innovation, efficiency, and excellence small businesses contribute to the industrial base, the OSBP&IE Team facilitates and fosters relationships to expand and strengthen the industrial base and national security.

As a result of its commitment to ensuring maximum practicable opportunities for small business participation across the agency, the OSBP & IE Team was recognized by the Office of the Under Secretary of Defense Acquisition and Sustainment for providing invaluable partnership and unwavering support in the demonstration of advancing the Department's FY23 Small Business Goals.

In further commitment to strengthening economic power through small business utilization, the OSBP&IE team participated in numerous educational, matchmaking, and training events, sponsored by the Department, to include APEX Accelerators Program, Small Business Development Centers, Native Hawaiian Organizations Association, and more, all to aid small businesses in their overall development, growth, knowledge, and defense industrial business expansion.

For FY24, the OSBP&IE Team looks to increase its internal footprint across the agency in further development of opportunities to strengthen the industrial base through small business engagement.

'Navigating the Clearance Process' campaign works to dispel myths



By Cheryl Jackson-Darden
Human Capital Management Office

In an effort to actively dispel myths surrounding the security clearance process, the Office of Diversity and Equal Opportunity (DEO) launched the "Navigating the Clearance Process" campaign in May 2023. Over the next seven months, this group of experts completed 10 "Navigating the Clearance Process" presentations for over 325 people. Additionally, the team was invited to present the campaign at the 2023 Out and Equal Summit, which is the largest Lesbian, Gay, Bisexual, Transgender and Queer + summit in the country with over 10,000 attendees.

Several Gatekeepers supported the 'Navigating the Clearance Process' campaign. (Courtesy photo)

The campaign featured panel discussions and presentations about the role of the Defense Counterintelligence and Security Agency (DCSA) in the security clearance process and common misconceptions about investigations and adjudicative guidelines. Each session included a panel of background investigations and adjudication experts, alongside a DEO moderator, discussing the source of these myths, many of which centered around sexual orientation, cultural differences based on nationality, foreign marriages, or dual citizenship. Experts also engaged in discussion about fallacies regarding security clearance denials due to perceived mental health, sexual orientation, foreign associations, financial dilemmas, disabilities, and other personal issues.

"Navigating the Clearance Process" is a nationwide educational outreach to ensure the public has an opportunity to ask questions, gain insights and increase awareness of national security roles. The campaign focused on reaching targeted groups such as students and recent graduates, veterans, transitioning service members, military spouses, and minority professional institutions. This initiative not only aligns to DCSA's strategic goals to recruit and retain high quality talent, but it also aligns with the White House Executive Order 13985 on Further Advancing Racial Equity and Support for Underserved Communities through the Federal Government. In fostering transparency about the security clearance process, the campaign has proven to be a useful recruitment tool to encourage job seekers to apply for federal jobs.

The team of DCSA employees who facilitate these sessions are passionate about their roles within the national security industry. Dr. Theresa Horne, DEO Director, created the campaign with assistance from others. Supporting the campaign as panel subject matter experts about the security clearance process were Special Agents in Charge Michelle Lake, Carrie Villegas and Robert Patterson; and from Consolidated Adjudication Services Chris Johnson and Tremell Munford.

Thus far in 2024, the campaign has approximately 24 events scheduled with consistent interest from schools, advocacy groups and military bases. The campaign will be sunset in December 2024. The Navigating the Clearance Process campaign provided transparency and clarity to the clearance process, supports national security recruitment, and highlights the importance of America's Gatekeepers.

DCSA Continuous Process Improvement program expands as Gatekeepers innovate, improve processes

By John Joyce
Office of Communications and Congressional Affairs.

QUANTICO, Va. – Defense Counterintelligence and Security Agency (DCSA) then Acting Director Daniel Lecce signed an instruction formally establishing policy and assigning responsibility for the agency's emerging Continuous Process Improvement (CPI) program on Feb. 4, 2024.

The new instruction, announced to the DCSA workforce three days later, comes on the heels of 20 Lean Six Sigma (LSS) Belt briefings on innovative CPI projects in September and December 2023, followed by another session in February.

It stems from Department of Defense (DOD) Directive 5010.42 and DoD Instruction 5010.43, aligning CPI to the DCSA Strategic Plan, employing LSS principles and other methodologies to improve cost effectiveness and efficiencies across the DCSA components.

The Gatekeepers who presented their certification projects comprise more than 140 Black and Green Belts trained and certified via the CPI program managed by the Chief Strategy Office (CSO) since January 2023.

In effect, they are pioneers who paved the way for the official adoption of DCSA Instruction 5010.43 and its procedures to implement the CPI program throughout the enterprise.

Since the inaugural LSS Green Belt training class, a wide representation of Gatekeepers across DCSA featured students from nearly every directorate engaged in the 40-hour training with its certified LSS Master Black Belt (MBB)-led instruction, group discussions, and practical exercises for real-world application.

The LSS Black Belt training class is a 120-hour training spread across three weeks which dives deeper into LSS methodology and more advanced application of statistical tools. The LSS Belt training prepares students to lead process improvement projects outside of the classroom and in the workplace using a data-driven, team-based approach to problem solving.

LSS prescribes an improvement process known as DMAIC; this acronym represents a five-step method for improving existing process problems with unknown causes as follows: define (the problem or performance gap); measure (quantify the problem); analyze (identify the cause(s) of the problem); improve (solve the root cause and verify improvement); and control (maintain the gains and pursue perfection).

Completion of a small-scale CPI project demonstrating the belt's knowledge and application of appropriate-level LSS tools is required for LSS Green Belt certification. A larger-scale, cross-directorate CPI project applying knowledge and application of these tools is essential for LSS Black Belt certification. All certifications are awarded by the CPI team's lead LSS MBB instructor, Narayanan Doraswamy.

"We are empowering Gatekeepers across the agency to take advantage of these training opportunities and obtain the necessary skills to identify and address pain points in their work areas—that's our bottom-up vision for the program," said Laura Bauer, DCSA CPI implementation lead. "We are also happy to see our top-down vision being fulfilled as senior leaders champion CPI while fostering DCSA's culture of innovation with many enthusiastically engaged at a CPI executive champion training event in February."

Bauer sees a top-down and bottom-up vision of innovative projects making incremental changes in myriad business processes to improve overall and specific efficiency and quality throughout the agency—near and long term.

This continuous application of CPI produces a moving picture of operations peppered with improved cost effectiveness, savings and efficiencies across the DCSA components (missions and staff). This common operational picture is based on policies outlined in the new instruction aligning CPI to the DCSA Strategic Plan as Gatekeepers employ LSS principles and other methodologies.

CPI program management authority and responsibility is delegated to the CSO to establish, administer, and manage the program, develop CPI capabilities, and to

issue subsequent CPI policies and procedures. DCSA components are responsible to identify and approve proposed CPI projects, and to build a cadre of trained Green Belt and Black Belt LSS practitioners.

"While housed in the CSO for day-to-day management, the CPI program is completely reliant on Gatekeepers," said Bauer, a CSO management and program analyst, who holds an LSS Black Belt. "It's critical for employees across the agency to be equipped with the training, knowledge and skills that will enable them to effect process improvement across the agency."

Moreover, employees are networking and collaborating to spread a culture of innovation applying new-found CPI capabilities that empower them to continuously identify customer requirements and increase flow in the delivery process while aligning products and service to better meet customer needs.

Consequently, Gatekeepers looking for ways to enhance business operations are suggesting ideas to improve efficiencies while evaluating current processes and finding ways to eliminate unproductive work.

"Our role is to teach Gatekeepers to fish, saying, 'hey, here's what you need to know, and this is how you can best address problems in your own workplaces.' Then, those who work in the missions or support offices that need a solution can more effectively apply CPI principles," said Bauer.

The primary CPI methodology is LSS, a proven framework focusing on enhancing value for the customer by using a team-based, data-driven process improvement approach to improve performance by systematically removing operational waste and reducing process variation. It combines Lean Management and Six Sigma principles to promote the use in work standardization and flow.

However, LSS is not the only CPI tool Gatekeepers have at their disposal. The CPI program has recently grown to include Scaled Agile training and certification programs.

"We have a whole community now across DCSA who are engaged and excited about process improvement," said Bauer, emphasizing that Gatekeepers can drive a culture of innovation at DCSA by taking advantage of these CPI program offerings.

"It's critical for employees across the agency to be equipped with the training, knowledge and skills that will enable them to effect process improvement across the agency."

Laura Bauer
DCSA CPI implementation lead

CPI's Scaled Agile Framework and Management

Agile is a project management methodology with an emphasis on continuous collaboration and improvement through iterative development – versus the more linear waterfall methodology. It involves breaking the project into phases and delivering solutions incrementally, where teams continuously cycle through discovery, planning, execution, and evaluation.

Since agile practices were first popularized by the Agile Manifesto in 2001, various agile frameworks emerged. The Scaled Agile Framework (SAFe) became the leading methodology for implementing agile practices at an enterprise scale. It's a body of knowledge that includes structured guidance on roles and responsibilities, how to plan and manage the work, and values to uphold.

In September 2023, Lecce commissioned the CSO to develop a SAFe training strategy based on roles and responsibilities and coordinated a comprehensive training program for delivery to key personnel.

The Agilist training offers an introduction to the foundations of SAFe and provides the principles and practices to confidently drive their transformation as lean-agile practitioners.

Participants will learn about topics that include lean-agile fundamentals, effective scaling, lean-agile principles, maximizing value, lean portfolio, seven core competencies, leadership skills, lead transformation, and lean portfolio management.

Agile training is also available for product owners and managers. It covers their tactical responsibilities and a customer-centric approach to building products to deliver more value, faster. These students will learn about scaled agile framework, lean-agile principles and values, collaboration with agile teams for delivery, and the delivery of continuous value.

Royal Reff, Office of Communications and Congressional Affairs, briefs his Lean Six Sigma Green Belt certification presentation in the Russell-Knox Building, Quantico, Va., Feb. 26 2024. (DOD photo by Christopher P. Gillis)

"Following training completion and passing of the certification exam(s), DCSA will have a trained and certified cadre of Agilists to support critical initiatives throughout the mission and enabling functions," said Bauer, who holds an Agile certification.

All trainings are provided by certified instructors and certifications are accredited through Scaled Agile Inc., which serves as an industry leading certification that validates DCSA employees' skills. Additionally, all trainings count toward continuing professional education credits.

Since CSO launched the SAFe training program in Fall 2023, there has been a high degree of interest from across the enterprise in pursuing these trainings and certifications.

At this point, 111 Gatekeepers have been trained with 82 receiving certifications as a result of the two DCSA course offerings: Leading SAFe and Product Owner/Product Manager (POPM).

"Our CPI team provided an overview of DCSA's CPI program with an introduction to the Scaled Agile Framework in addition to a discussion of the Lean Six Sigma training and certification program," said Bauer. "The goal of this training was to ensure each directorate's senior leader had an understanding of targeted CPI methodologies with associated champion responsibilities and best practices for instilling a culture of continuous improvement and innovation at DCSA."

The CSO CPI team strives to incorporate feedback, wherever possible, into future CPI offerings utilizing the feedback received from former students and their champions. The team is available to provide ongoing coaching while supporting LSS certification and other CPI efforts across the enterprise

Agency reinforcing diversity, equity, inclusion in learning environment

By George Robinson
Office of Diversity and Equal Opportunity

The National Center for Credibility Assessment (NCCA) designed its training programs with a focus on organizational culture as the foundation. Based in Fort Jackson, S.C., the NCCA hosts a diverse range of individuals in its courses, and actively invites stakeholders and partners to send personnel from their respective agencies to act as sample subjects throughout training. This collaborative effort ensures that the program maintains fairness and inclusivity, providing a wide array of experiences and perspectives for examiners-in-training. Moreover, the NCCA's partnership with the DCSA Office of Diversity and Equal Opportunity (DEO) underscores their shared commitment to promoting diversity, equity, inclusion, and accessibility in the learning environment.

Diversifying student pool

To ensure that polygraph examiners have a wide range of experiences and viewpoints, the NCCA relies on Fort Jackson to provide soldiers to the polygraph examiner labs. More than half of all Army recruits attend basic training and more than 60% of all female soldiers go through basic training at Ft. Jackson. NCCA includes a diverse group of soldiers, each with their own unique backgrounds, to assist with labs and hands-on training opportunities throughout the intensive 12-week program. This approach helps future examiners gain practical experience in dealing with different cultures and backgrounds in a real-world setting.

Cultivating inclusive culture

Additionally, NCCA encourages anonymous feedback from staff and students by providing an environment for people to openly share their thoughts and experiences through surveys, open door policies, and consistent check-ins for staff, trainees and volunteers. This level of open conversation supports inclusivity and enhances stakeholder experience. By actively involving and appreciating the viewpoints of its members, the NCCA aims to establish an environment where everyone's voice matters and feels respected.

Collaboration with DEO

To reinforce inclusion, DEO sought to enhance the learning experience of the polygraph examiner course by incorporating the Unconscious Bias and Cultural Inclusivity (UBCI) training, developed by the DEO Director Dr. Theresa Horne,, into the NCCA's accredited training plan. The UBCI training delves deeply into how biases, stereotypes, and cultural awareness may impact examiners and their duties. By training on cultural awareness, examiners can enhance public facing communication and increase the ease of collecting information from subjects.

Looking ahead

The NCCA and DEO are working to incorporate UBCI training as an ongoing component at NCCA, setting a precedent for high-quality, real-world training that explores self-awareness, cultural and environmental differences.

‘FOC Huddle’ opportunity to address topics of interest, share best practices

By April Rodriguez-Plott
Field Operations

Industrial Security Representatives (ISRs) interface, engage and oversee the implementation of the National Industrial Security Program in industry. ISRs play a vital role in support of the cleared defense industrial base as well as serving a critical team player for national security. ISRs work with cross-mission colleagues Information Systems Security Professionals, Counterintelligence Special Agents and Background Investigator Special Agents to collaborate, share information and keep the missions moving forward.

The Western Region (WR) Industrial Security (IS) Leadership Team takes time out of a busy week of operational activities for a team building dinner on December 13, 2023, at the Jazz Kitchen restaurant along the boardwalk of the Happiest Place On Earth, in Anaheim, CA. Bottom Left, up and to the Right: FOC David Cohen, FOC Nicole Cooper, CUI Action Officer Lillian Benitez, FOC Joe Webb, RMD IS Nadja L. West, CUI Action Officer Matthew Sergen, DRMD IS April Rodriguez-Plott, FOC Kevin Flowers, and FOC Jon Laahs.

While the cross-discipline teams are in the field day after day executing mission duties, Nadja West, Regional Mission Director, Industrial Security Western Region, found it essential for Field Office Chiefs, the first line supervisors within Industrial Security field offices, to have dedicated in-person meetings to collaborate with headquarters elements, address planning and operations, and orient to the needs of the industrial security workforce in Western Region (WR). As a result, the Field Office Chief (FOC) Huddle was established, which is often referred to as the FOC Huddle.

On a quarterly basis, each FOC has an opportunity to host and create an agenda of topics and solicit guest speakers because they are closest to the needs of the field and the huddle offers a venue to address topics of interest that have an immediate impact on the industrial security mission. For example, during the December huddle, colleagues from the Enterprise Security Operations Controlled Unclassified Information (CUI) Branch provided a briefing regarding CUI efforts and engagement with industry as well as insights from the CUI pilot from the first quarter of FY24. Creating a space to connect with colleagues in other industrial security focused mission areas offers a unique opportunity to understand on-going agency initiatives and provides a connection point for local leaders in this quickly growing and evolving organization.

The huddle also dedicates time to mission planning. The FOC team reviews key performance goals, execution rates, operational impacts, such as staffing, and allows for a discussion of metrics. Orienting to business planning and year-to-date actuals offers the leadership team an opportunity to understand how other field offices are postured to align with regional goals and share best practices. This may result in coordinating temporary duty support for one another or assessing ISR workforce bandwidth considering both mission goals and the workforce needs.

A popular segment during the FOC huddle is called a “A Day in the life of an ISR.” During this segment made popular by Field Office Chief Kevin Flowers, San Franscico field office, a group of ISRs are invited to join the huddle to speak candidly about culture, operational tempo, challenges and share their experiences. The purpose of this session to hear about work-life balance from their perspective and how leadership can help. The team uses this insight to understand communication gaps, assess needs of the field and continuously work to fill identified gaps.

The huddle creates the time for operational discussions, cross-mission area briefings, and team building to promote a positive team culture, trust, and common strategic purpose and direction for region IS leaders, facilitating the ability to accomplish field office, region, and agency goals. It provides a chance to connect, reflect and plan how to best lead and support industrial security field operations.

Nurturing partnerships critical in protecting national security

By Ryan Franklin
Field Operations

With approximately 12,500 cleared facilities authorized to access classified information under DCSA's security oversight responsibilities in the National Industrial Security Program (NISP), a critical component of DCSA's established mission is continuous engagement with industry partners. Collaboration and partnership with industry is critical in developing appropriate risk-based methods used to help improve security programs across the NISP, to counter the evolving threat facing the defense industrial base, and to protect national security. A great way to foster productive relationships with industry partners is by participating in industry-hosted events and conferences.

The FFRDC/UARC Security Council was founded to share information and best practices amongst its FFRDC (Federally Funded Research and Development Centers) and UARC (University Affiliated Research Centers) members and to serve as a voice to government as to the modification of existing and the creation of new security policies and implementing guidance. FFRDCs and UARCs perform a unique mission in support of their government sponsors by researching, developing, advancing, and maintaining essential engineering, science, mathematics, and applications important to the U.S. government.

In support of its mission, the Council hosts semi-annual security conferences to gather and discuss various topics pertaining to industrial security.

During the most recent council meeting, participating organizations shared best practices and information on hot topics pertaining to industrial security, including controlled unclassified information, export controls, insider threat, physical security, information systems, personnel security, policy and operations, and special programs. Senior Industrial Security Representative Najah Basyouni and Industrial Security Representative Kenneth Kisby Jr., both from the Alexandria 1 Field Office, participated in working sessions, providing additional guidance and feedback on policy requirements and security best practices implemented by the FFRDC/UARC security community to maintain effective and compliant security programs. DCSA industrial security representatives also provided feedback and guidance to personnel seeking specific direction in on-going issues and hot topics.

Assistant Director for Industrial Security Matthew Redding served as a keynote speaker, presenting on the way forward for DCSA's Industrial Security mission, receiving questions from conference participants and addressing their concerns. Conference attendees also had the chance for one-on-one conversations with Redding to discuss current challenges facing the industrial security mission, the defense industrial base, and industrial security field personnel, highlighting specific challenges and accomplishments in the Mid-Atlantic Region. Booker T. Bland Jr., Deputy Assistant Director, Enterprise Security Operations within IS, presented on controlled unclassified information updates, and Project Manager Chuck Tench participated in a panel discussion regarding updates relating to National Background Investigation Services.

Nurturing effective partnerships between DCSA and cleared defense contractors in the NISP are vital to protecting national security information and assets critical to their contributions in support of U.S. Government missions and objectives.

First established during World War II, Federally Funded Research and Development Centers are independent, not-for-profit, private-sector organizations that are established and funded to meet special long-term engineering, research, development, or other analytic needs that cannot be met as effectively by government or other private-sector resources. FFDRCs are operated, managed, and/or administered by universities, or privately organized not-for-profit corporations, through long-term government contracts.

University Affiliated Research Centers are all non-profit research organizations affiliated with a university and have a set of core competencies—areas of domain expertise or specialization - that are tailored to the long-term needs of the Department. DoD's long-term strategic relationship with UARCs requires them to provide and maintain advanced and sophisticated engineering, research, and/or development capabilities essential to the Department's mission and operations.

The benefit of an FFRDC or UARC is that there is no profit motive, is answerable only to the government customer and has no vested interest in particular technologies or solutions.

DCSA leaders, team building events inspire Gatekeepers on 'Leap into Wellness Day'

By John Joyce
Office of Communication and Congressional Affairs

What do cornhole, line dancing, family feud, treasure hunts, Jenga, nature walks, baby picture guessing, healthy recipe swaps, chats over coffee, golf, and board games have in common?

The answer involves the Defense Counterintelligence and Security Agency (DCSA) employees who engaged in those activities or other 'Leap into Wellness Day' team building exercises virtually and in person across the nation to relax, recharge and learn something new related to wellness while getting to know their DCSA colleagues better on Feb. 29.

"In today's fast-paced and demanding work environment, it's easy to get caught up in the never-ending cycle of tasks, deadlines and responsibilities," said Salome Smalling, enterprise knowledge management analyst at the DCSA Chief Strategy Office while reflecting on the day's activities. "We need to reevaluate our approach to work and wellness. The wellness Leap Day event was a great reminder for us to take a step back and practice self-care, which will bring more joy, rest and balance. The benefits of incorporating wellness days extend beyond the individual to the workplace itself. When we practice self-care, it offers a well-balanced environment, provides creativity that flourishes, sharpens problem-solving skills, and builds strong interpersonal relationships, both personal and professional."

The Quantico Investigative Field Office, Background Investigations-Field Operations, gathers at Government Island, Stafford, Va., for a nature walk during Wellness Day.

The Industrial Security San Francisco Field Office practiced their golf swings at Top Golf in San Jose, Calif, on Wellness Day. In the front row is Senior Industrial Security Representative June Kim. Middle row (from left to right) is Andrea Coelho, Nicole Siebe, and Industrial Security Representative Janet La Salle. In the back row is Field Office Chief Kevin Flowers.

Wellness-related briefings and engagement among DCSA teams and colleagues reflected the agency's commitment to caring for the well-being of the workforce. Gatekeepers connected with each other in various events, reviewed available wellness resources, and celebrated the achievements of their co-workers who live DCSA's values.

"We at DCSA are a people focused and values driven organization, that's who we are," said then-DCSA Acting Director Daniel Lecce. "In this era of post-COVID telework and remote work, sometimes we lose important connections. Take the time to connect and take care of each other. What is your character? It's vitally important to maintain and live your values. Not when people are watching, when people aren't watching. That is your character. Your integrity."

The day's happenings, which included time in the afternoon for local team building activities to enhance interpersonal relationships, supported two objectives in the agency's Unity of Effort strategic goal:

• Build an integrated agency that operates holistically as a single enterprise.

• Sustain a strong culture of innovation, strong partnerships, and inclusivity.

"I know how difficult it can be to juggle wellness with all the competing demands of work and daily life," said DCSA Chief of Staff Ellen Ardrey in discussing a positive Gatekeeper experience. "It fosters a sense of wellness and work-life balance, community, camaraderie and trust in fellow Gatekeepers. Wellness is vital to understanding our purpose and unique roles in executing DCSA's mission."

Ardrey assured her audience that DCSA's inaugural Wellness Day and the various activities won't be the end of the conversation about wellness, camaraderie and a holistic Gatekeeper culture.

"This is just the starting point of what we hope will continue throughout the year," she said. "It's going to be an ongoing process to find the best ways to encourage wellness as part of our Gatekeeper culture as we continue our cultural transformation.

"This journey to build our culture remains the agency's top priority," she continued. "A positive Gatekeeper experience will look different for everyone and we're seeking to give employees a sense of wellness, a community of trust. That's a big one—trust, purpose, fairness, optimism and integration—and everything you do with DCSA informs your Gatekeeper experience and influences those around you. It's every minute of your DCSA experience, including the interactions you have with your peers, subordinates and senior leaders every time you go to training or a meeting. It's the tangibles and a lot of the intangibles - the feelings that you have coming to work and interacting with folks."

Daniel Moore, Program Executive Office, stops during his bicycle ride around Lake Montclair in Dumfries, Va.

The intangibles, job satisfaction, a sense of accomplishment, workplace optimism, communication, innovation and engagement, are key to Gatekeepers' psychological wellbeing, motivation, productivity, collaboration and teamwork.

The two hours of team building activities kicking off Wellness Day were followed by a town hall featuring DCSA leaders and video testimonials by five employees who described their perspectives of Gatekeeper values—mission, people, service, integrity and innovation—in action.

The employees selected to give Gatekeeper testimonials on living DCSA's values were among 24 candidates nominated by their supervisors for the opportunity to present a five-minute video address on a specific Gatekeeper value. "These Gatekeeper spotlights are outstanding," said Lecce. "We chose them to go over our values and what they mean to them personally."

In their TED talk-style approach, Luke Baxter, Carol Banks, Annalee Smith, Ashley Dalisera and Sean Lavigne, projected positivity and sincerity while describing how they prioritize their value in their respective Field Operations, National Center for Credibility Assessment, and Program Executive Office workplaces.

Events throughout the day encouraged healthy lifestyles that enhance the quality of work-life and productivity. Meanwhile, Gatekeepers initiated or renewed friendships and connections with each other.

"We enjoyed breakfast together where we discussed non-work-related topics and ways we might better improve our understanding of our strengths and interests professionally and personally as we grow as a field office," said one of 659 employees who provided feedback via an anonymous survey after the day's events. "This was very encouraging. We also spent an hour playing Topgolf, which built great camaraderie both in our field office, but also with our collocated field office."

According to the survey, psychological safety and the agency's initiatives to improve wellness and work-life balance were favorite Wellness Day discussions. Psychological safety is the single most important characteristic for successful teams and leads to decreased turnover, increasing effectiveness while empowering wellness, according to DCSA Human Capital Management Office leaders, Dr. Dana Sims and Alex Rivera who briefed the agency on Wellness Day.

They emphasized that psychological safety boosts team performance because employees feel secure enough to share diverse ideas and perspectives, resulting in improved problem-solving and decision-making. They added that it enhances the ability to handle change and uncertainty since the ability to voice concerns and suggestions helps employees navigate change where flexibility and responsiveness are crucial in fast-paced or uncertain environments.

In relation to psychological safety, Lecce spoke about the five pillars of wellness while emphasizing the importance of family wellness in addition to emotional, physical, spiritual and social wellness.

"What is wellness," he asked, answering his question: "It's body, mind, and spirit. All three are connected."

Emotional wellness involves being self-aware and able to handle emotions constructively. Physical wellness can be achieved through proper nutrition, physical activity and flexibility. Spiritual wellness means finding meaning and purpose in life.

There's also social wellness which involves maintaining harmonious relationships with others. Family wellness relates to supporting children and support strategies for spouses, partners or parents while maintaining the health and unity of the family.

"We expect a lot out of our workforce, but you have got to take care of your family," said Lecce. "All of us regret things that we've done because of work. In five years, no one will remember the long days that you're working and the overtime, but your children will remember if you missed their party. They will remember if you missed their gymnastics meet. They will remember if you missed a church event.

Gatekeepers from the San Diego Field office - San Diego North County and San Diego-Camp Pendleton teams, hike the Piedras Pintadas Trail, San Diego, Calif., on Wellness Day.

"There is nothing that's too important that you cannot take time for your family, and you need to do that," he continued. "This is part of that journey I'm talking about when we talk about mindfulness in your spirit. Your family and your friends are directly connected with it, and how important that is to us."

From left to right, Joel West, Esquire, Maria Gales, Ryan Norwood, and Samantha Barbarczuk, Counterintelligence and Insider Threat Directorate, complete the Rubber Ducky Memory Challenge during Wellness Day.

Career broadening, greater understanding of mission goals of new program

By Dante Swift
Office of Communications and Congressional Affairs.

Since the inception of the Defense Counterintelligence and Security Agency (DCSA), one of the primary goals has been to build a talented, diverse, and inclusive workforce that could meet the demands of DCSA's evolving mission. For many existing employees, there has been a disconnect in understanding how their individual role intertwined with multiple mission areas during periods of collaboration.

In response to several employees expressing an interest in learning about and understanding the full scope of DCSA outside of their job series, the DCSA Human Capital Management Office (HCMO) created and implemented the Career Broadening Program (CBP) in 2023. "We saw great interest from organizations willing to host opportunities," said Dr. Randy Maraj, one of HCMO program managers who developed the CBP. "Organizations were very supportive of bringing in employees and providing mentorship and on-the-job training."

The HCMO and DCSA leadership agreed to focus on a specific segment of the workforce, targeting full performance level, non-supervisory GG-12/13s, who execute in key mission areas but may have limited opportunities for professional and personal development within their series.

"It was important to provide this essential group of employees a broader view of the agency," said Alex Rivera, Chief of the Employee and Leadership Development Division in HCMO. Exchanging knowledge cross-agency builds an integrated workforce, while exposing opportunities for those who seek change but enjoy contributing to the DCSA mission.

The length of the program sparked discussions, as DCSA and HCMO leadership wanted to ensure that CBP participants gained experience and perspective while not impacting their home organizations tremendously. To achieve these objectives, a duration of 179 days was set and in January 2023, the CBP program began soliciting volunteers for a pilot cohort.

"While we know we can continuously make the program stronger, the best news was that the personnel involved found it to be a valuable experience and recommended it be continued."

Barbara Phelps
Human Capital Management Office

"The temporary loss of a member will impact our pending workload; however, I view the short-term loss as minimal considering the positive outcomes Agency wide from an employee's participation," said Cynthia Vazquez, the Deputy Regional Mission Director of the San Diego Field Office, of the CBP participant that came from her office.

As the pilot program concluded, preparations began for the first cohort. Utilizing surveys and focus groups with participants and supervisors, the CBP team gathered feedback and identified what went well and which areas needed improvement.

"While we know we can continuously make the program stronger, the best news was that the personnel involved found it to be a valuable experience and recommended it be continued," said Barbara Phelps, the other HCMO program manager who was instrumental in implementing the CBP.

Fiscal Year 2024 welcomed the first cohort, which began in November 2023. With agency-wide attention and support, the CBP was welcomed as an official staple of professional and personal development for DCSA employees. The growth of the program from the original 10 positions to 24 new opportunities confirmed both the desire of the workforce to have opportunities to expand their skillset and the benefits cross-collaboration brought to hosting directorates and offices. With an abundance of applicants, Cohort #1 went live with 21 participants filling 18 roles (some roles allotted two employees) across the entire DCSA enterprise.

Jillian Lien, a Special Agent in the Virginia Beach Field Office, Background Investigations (BI), Field Operations, is currently serving as a Program Manager for CDSE as part of Cohort #1 of FY24. She stated, "The Career Broadening Program is an incredible opportunity that has deepened my appreciation of DCSA and has shown me how different components contribute to one greater mission."

"Being part of the CBP broadened my perspective of DCSA as a whole," said Special Agent Carol Banks, San Diego Field Office BI Field Operations. "More importantly, it helped me renew my motivation to influence change and to be an active part of DCSA's transformation efforts." Banks served as a Strategic/Resource Planning Action Officer in the Chief Strategy Office for her rotation.

> "... it helped me renew my motivation to influence change and to be an active part of DCSA's transformation efforts."
>
> *Special Agent Carol Banks*
> *San Diego Field Office*
> *Background Investigations*
> *Field Operations*

The CBP is described as a tool designed to increase recruiting and retention efforts. With the evolving mission areas and the advancements in tech and cybersecurity, DCSA has entered a new era that requires more attention to our purpose. "My motivation to participate in the program was not necessarily to change career fields, but to be exposed to other aspects of DCSA. A string can be strong, but if you tie the strings together, such as in a braid, then it makes the fabric stronger," said Special Agent Michelle Lake. "The greatest benefit that I learned from this program is that we have amazing strings (employees), and when we are banded together, we are hard to break. As Gatekeepers, we just become stronger and more resilient." Lake served as an Equal Employment Opportunity Specialist: Special Emphasis Program Manager, Trainer, for the Office of Diversity and Equal Opportunity.

"As a background investigator, I only see one facet of the agency. This detail provides opportunities to collaborate with individuals from different disciplines," said Special Agent Candace Truong, San Diego Field Office, BI, Field Operations. "Integration of all mission areas creates a continuous link that makes the agency more resilient and effective in protecting national security." Truong is currently working in the Front Office as an Action Officer

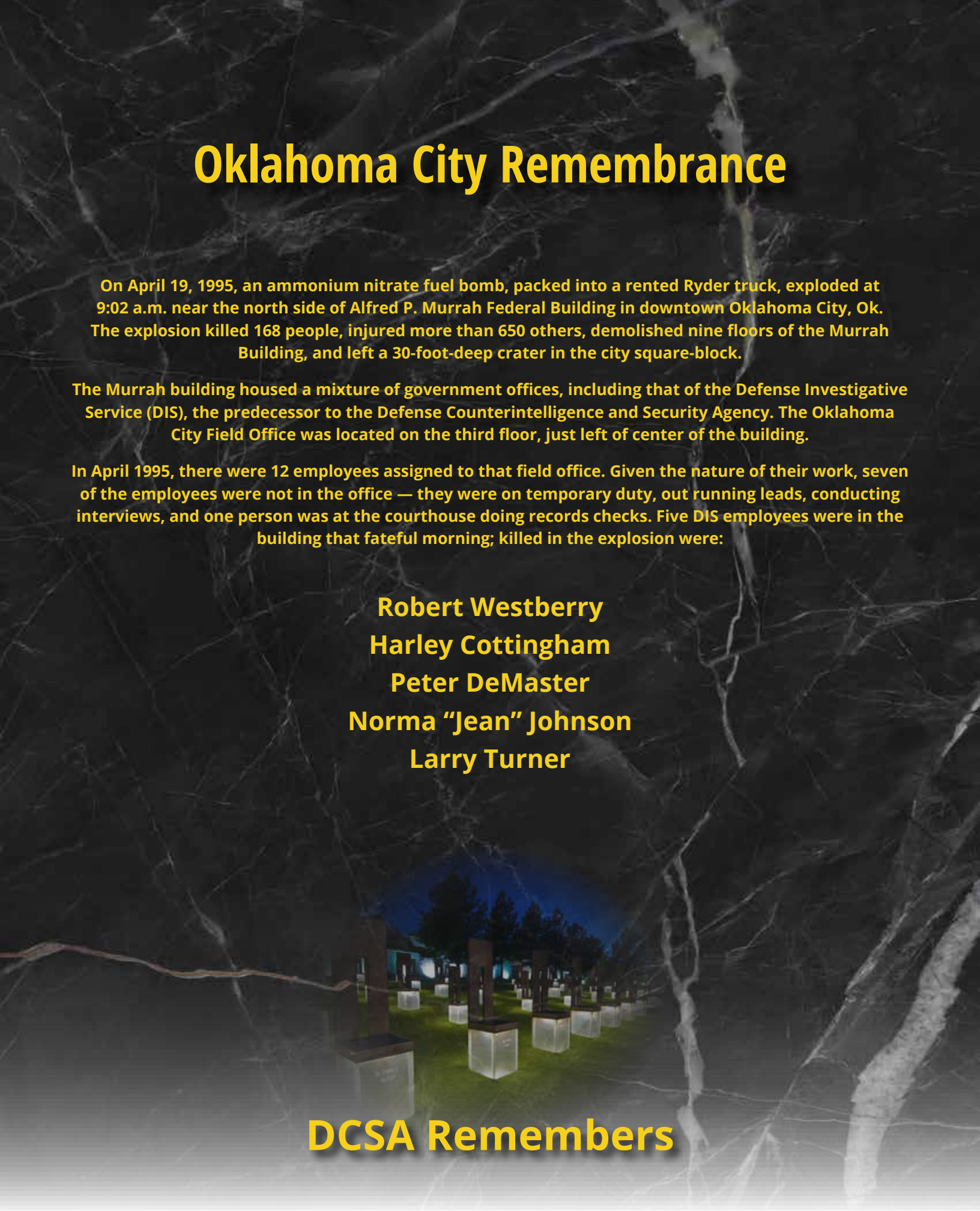
Oklahoma City Remembrance

On April 19, 1995, an ammonium nitrate fuel bomb, packed into a rented Ryder truck, exploded at 9:02 a.m. near the north side of Alfred P. Murrah Federal Building in downtown Oklahoma City, Ok. The explosion killed 168 people, injured more than 650 others, demolished nine floors of the Murrah Building, and left a 30-foot-deep crater in the city square-block.

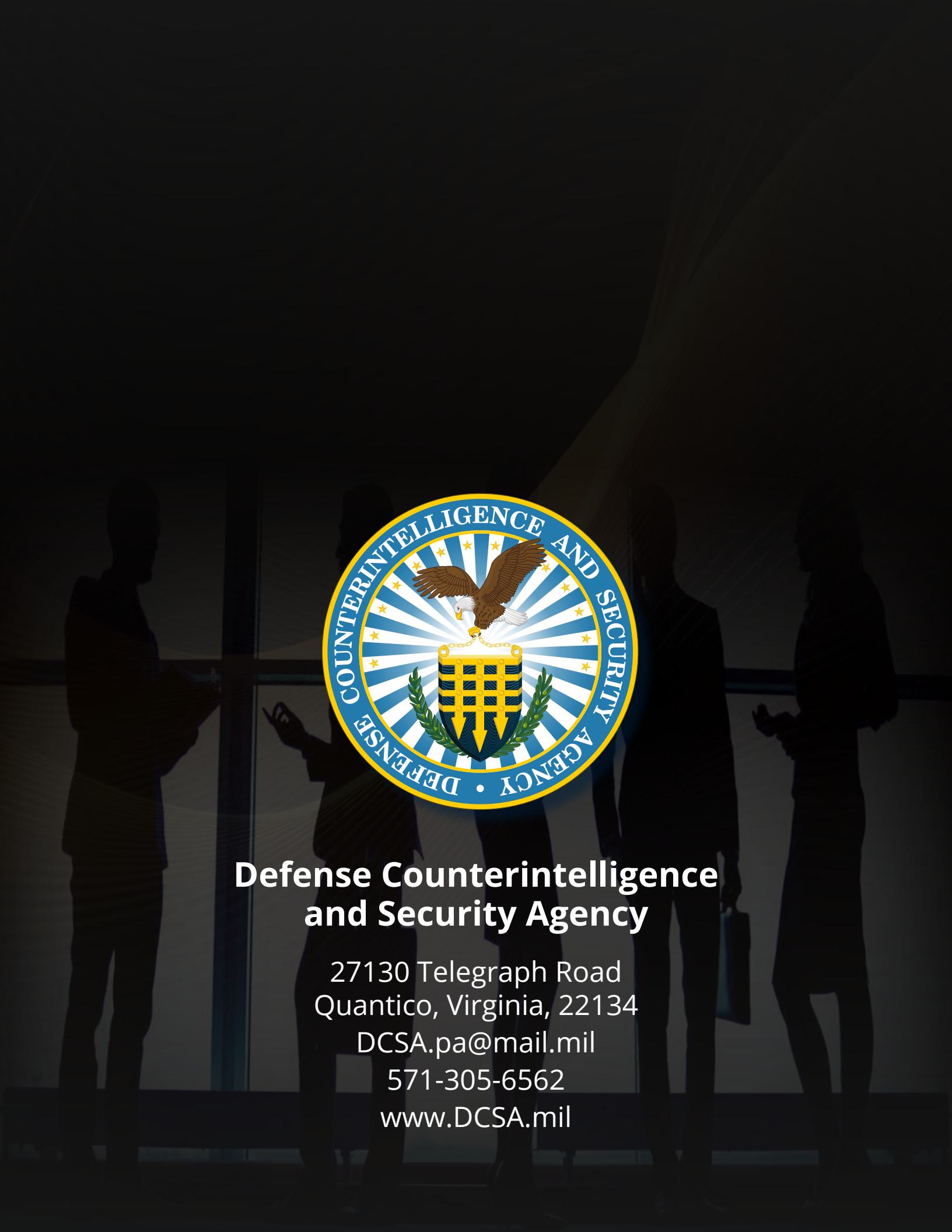
The Murrah building housed a mixture of government offices, including that of the Defense Investigative Service (DIS), the predecessor to the Defense Counterintelligence and Security Agency. The Oklahoma City Field Office was located on the third floor, just left of center of the building.

In April 1995, there were 12 employees assigned to that field office. Given the nature of their work, seven of the employees were not in the office — they were on temporary duty, out running leads, conducting interviews, and one person was at the courthouse doing records checks. Five DIS employees were in the building that fateful morning; killed in the explosion were:

Robert Westberry
Harley Cottingham
Peter DeMaster
Norma "Jean" Johnson
Larry Turner



DCSA Remembers



Defense Counterintelligence and Security Agency

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