

Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper



SF862020



Volume 3, Issue 3

10/10

Sections complete

- Information about you ✓
- Your history ✓
- Relationships ✓
- Citizenship ✓
- Military history ✓
- Foreign associations ✓
- Financial record ✓
- Substance use ✓
- Investigative and criminal history ✓
- Psychological and emotional health ✓
- Review and submit ✓
- Additional Comments
- Review
- Submit
- Print

All required fields are complete

Not a guarantee of acceptance, but all required fields are complete.



Please sign the releases below and submit your form

After completing this form and any attachments, you should review your answers to all questions to make sure the form is complete and accurate, and then sign and date the following certification and the attached release(s).

Download a Draft PDF For Review

Certification

Release of Information & HIPAA

Credit reporting disclosure

Submit your SF-86

**DCSA announces transition to new
'intuitive' NBIS eApp background
investigation process**

IN THIS ISSUE

ASK THE LEADERSHIP

**AGENCY PRESENTS 19
COGSWELL AWARDS**

**DCSA SENIOR LEADER RECEIVES
PRESIDENTIAL RANK AWARD**

IN THIS ISSUE

FROM THE DIRECTOR	3
DCSA ANNOUNCES TRANSITION TO NEW 'INTUITIVE' NBIS EAPP BACKGROUND INVESTIGATION PROCESS.....	4
NBIS: A ONE-STOP-SHOP SYSTEM FOR END-TO-END PERSONNEL VETTING	6
ASK THE LEADERSHIP	8
DCSA RECOGNIZES THE BEST IN INDUSTRIAL SECURITY; 19 FACILITIES RECEIVE COGSWELL AWARDS IN 2023.....	11
DCSA SECURITY PROGRAMS CHIEF PRESENTED WITH DISTINGUISHED PRESIDENTIAL RANK AWARD	12
'INTEGRATE' TABLETOP EXERCISE FOCUSES ON GAPS IN INFORMATION SHARING, PROPOSES SOLUTIONS.....	13
ENTERPRISE GOVERNANCE FRAMEWORK SUPPORTS EFFICIENT DECISION-MAKING FOR AGENCY	14
TO MAINTAIN SPED CERTIFICATIONS, ACQUIRE REQUIRED PROFESSIONAL DEVELOPMENT UNITS	15
DCSA EMPLOYEES, TEAMS HONORED AT DIRECTOR'S AWARDS AND RECOGNITION PROGRAM CEREMONY	16
RECOGNIZING 50 YEARS OF SERVICE, AGENCY PLACES WREATH AT TOMB OF THE UNKNOWN SOLDIER.....	20
NCCA UNVEILS COLLABORATIVE MULTI- DISCIPLINARY LAB CAPABILITY TO IMPACT NATIONAL SECURITY	22

Vol 3 | ISSUE 3

DCSA Gatekeeper

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

DCSA LEADERSHIP

William K. Lietzau
Director

Juli MacDonald
Chief, OCCA

Cindy McGovern
Managing Editor

Elizabeth Alber
Editor

John J. Joyce
Staff Writer

Christopher P. Gillis
**Digital Content
Specialist**

Tony Trigg
**Layout, Editing and
Design**

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

All pictures are DOD photos, unless otherwise identified.



FROM THE DIRECTOR

As we move through the summer months, the end of the fiscal year looms large. And with it comes another year of transformational change for DCSA. As the pages in this issue illustrate, DCSA is poised in fiscal year 2024 to

deploy key functions of NBIS — the end-to-end personnel vetting system forming the backbone of Trusted Workforce 2.0. This is but one example of the continued maturation and transformation of the Agency while we solidify its culture.

Although I am pleased that we are able to highlight the achievements of our incredible workforce, this issue comes at a bittersweet moment for me. As many have now heard, I recently announced to the workforce my decision to retire in the coming months — so this may be my final introductory note for the Gatekeeper. With that in mind, I would like to share with you my thoughts on DCSA's journey over the past three years and why I prepare to leave with substantial optimism for its future.

In contrast to the early days following the merger, when the Agency grappled with the turmoil of major transitional changes, today's DCSA has transformation and innovation built into its DNA. Hitting strategic milestones is now commonplace for our workforce. We do so not because change is mandated by an outside force, but rather because we have inculcated the Agency's vision, mission, and core values as a part of everything we do.

As I reflected on how far we have come as an Agency, I went back to the first Gatekeeper publication from January 2021. Besides adopting DCSA's new moniker of "America's Gatekeeper," that inaugural issue encouraged the shedding of legacy identities as we sought to establish a new security culture promoting unity of effort across DCSA. In this regard, we have learned that our core values play an essential part in shaping and defining our culture.

Besides being driven to innovate, DCSA's workforce is laser-focused on our mission; it cultivates and invests in its people; it exhibits an unwavering regard for integrity; and it is passionate about service to this country.

With these values firmly entrenched in the Agency's workforce and culture, I leave DCSA with confidence in the future of our nation's security. But just like courage is necessarily accompanied by fear, in this case confidence is challenged by the existential nature of today's threat. Nearly three years ago, "Gatekeeper" was selected as the overwhelming favorite appellation for the new publication — because it is the title we each claim. "Glamour," "wealth," and "power" are not terms that align with Gatekeeper. But "strength" and "duty" are. And the import of DCSA's mission has never been greater.

Indeed, "America's Gatekeeper" is best described as a nom de guerre as opposed to a nickname. DCSA and its Gatekeepers are at the tip of the spear; we are at war every day fighting to protect our workforce, our industrial base — including its most critical technologies — and our defense supply chain. These represent our nation's crown jewels, and they must be protected with the utmost vigilance. We, as Gatekeepers, must be on watch, day and night, against this very real and persistent threat.

In announcing my retirement, I mentioned being overwhelmed with pride and gratitude at having been part of this Agency; there is no community with whom I would rather affiliate as I close out my government service than the Gatekeepers who comprise DCSA. As I pass the baton to the next Director, I rest assured that today's unprecedented threat is more than matched by the unprecedented inspiration and dedication of DCSA's workforce.

Thank you for your exemplary service to each other, our Agency, and this great Nation.

William K. Lietzau
Director,
Defense Counterintelligence
and Security Agency

DCSA announces transition to new ‘intuitive’ NBIS eApp background investigation process

By John Joyce

Office of Communications and Congressional Affairs

The National Background Investigation Services (NBIS) Electronic Application (eApp) — a new and more user friendly interface for applicants submitting standard investigative forms — is replacing the Electronic Questionnaires for Investigations Processing (eQIP) functionality. NBIS customer agencies are required to begin using eApp to initiate applications, and its partner system, NBIS Agency, by Oct. 1, 2023.

The ‘NBIS eApp Transition’ Federal Investigations Notice (FIN) 23-02 signed by DCSA Director William Lietzau describes the shift to eApp as a “sequential event to meet mandated requirements to transition from legacy systems to the NBIS technology solution.”

The onboarding — conducted in scheduled phases — and transition to NBIS eApp and NBIS Agency as the entry points for background investigation applications is already 93% complete among federal agencies with 11% of federal organizations completing the transition in full and no longer using eQIP. DCSA leaders report that industry is also making good progress in transitioning from eQIP to eApp.

NBIS Agency is the new application allowing government security managers and industry Facility Security Officers (FSOs) to process background applications and manage them through the investigation process. Based on modern, simple design elements, eApp makes the application process via standard investigative forms more intuitive and easier to use for applicants initiating a background investigation.

Standard investigative forms initiate the background investigation and adjudication process for security clearance decisions or enrollment in the DCSA Continuous

Vetting program — an ongoing screening process to review the background of individuals with access to classified information.

“All federal customer agencies should be transitioning users from eQIP accounts to NBIS eApp for the purposes of completing and processing investigative forms (SF86, SF85, SF85P, SF85PS etc.) to support request for background investigations or enrollment in Continuous Vetting,” according to the Federal Investigations Notice. “DCSA agency liaisons and NBIS onboarding teams are available to assist agencies in this transition.”

NBIS customer agencies and Industry are required to begin using eApp to initiate applications, and its partner system, NBIS Agency by Oct. 1, 2023. To support this timeline for adoption, DCSA established a support team for both Federal and Industry to assist in the transition process. The scheduled support will be prioritized by group depending on an organization's complexity, requirements, and preparedness, among other considerations. At this point, 107 Federal agencies have started using eApp (applications) and NBIS Agency (security management). Industry is just beginning to use the system as NBIS matures more Industry-specific capabilities and push for approximately 13,000 Industry organizations to self-onboard to the NBIS system.

“As needed, additional guidance regarding eQIP decommissioning activities, such as handling of cases in progress, will be addressed in forthcoming investigative notices,” Lietzau explained in FIN 23-02. “We look forward to continuing our partnership as we transition to NBIS. We value your efforts to date and appreciate your continued support through this process. We are here to support.”

Applicants and employees will discover improved access and transparency — compared to the legacy applications — when signing into the eApp portal to initiate an investigation.

The e-App subject portal will allow better tracking of individual case status. The application itself will be easier to use while providing better information for vetting professionals. Applicants and employees will have the ability to save their applications more easily.

Moreover, eApp improves the overall user experience for applicants step by step throughout the application process from initiation to adjudication as follows:

- eApp is designed to improve the most challenging part of the background investigation process: the application.
- The SF86 investigation application legacy process is replaced with a smart, simple eApp platform guiding users through the application quickly.
- Efficient and effective eApp features include timeline validation, automatic address checks, real-time feedback, and section previews.
- Real-time validation and help means less errors and less time required to get through the application process.

The eApp portal's technology improvements feature a modern, user-friendly initiation with more intuitive and logical groupings; applicants only see questions relevant to them; auto saving; U.S. Postal Service address validation to reduce error rate; timeline validation to reduce incomplete or inaccurate input; real-time validation and error detection to catch errors sooner in the process reducing

resubmission delays; consistent layout and visual design for smooth user engagement; and additional user help features built in system to provide clarity for users.

The NBIS eApp Transition Federal Investigations Notice 23-02 is posted on the DCSA public website.

DCSA liaison officials and NBIS help desk representatives are available to assist agencies in this transition. For assistance or questions, visit <https://dcsa.servicenowservices.com/>.

Additional NBIS eApp resources are available via these links:

- User Account Service Now Submission Portal: <https://dcsa.servicenowservices.com/csm>
- Self-Help Training Modules: <https://nbistraining.countermeasures.com/courses/home>
- Knowledge Articles: https://dcsa.servicenowservices.com/csm?id=kb_home



INITIATION



QUESTIONNAIRE



INVESTIGATION



ADJUDICATION



CONTINUOUS VETTING

NBIS: A one-stop-shop system for end-to-end personnel vetting

By Lena Burns

Personnel Security

In 2019, the Defense Counterintelligence and Security Agency was established bringing the critical personnel vetting missions together, under one umbrella. In 2022, the Personnel Security Directorate was formed to further integrate personnel vetting operations at DCSA.

Assistant Director of Personnel Security Dr. Mark Livingston is committed to delivering efficient and effective background investigation, continuous vetting, and adjudication services to safeguard the federal and contractor workforce's integrity and trustworthiness.

"The national security work DCSA executes every day is paramount to the continued success of the cleared population," said Livingston. "Our motto is status quo will not work. We are always looking to improve even what is working well."

The next step, and one of the agency's top priorities, is to provide an information technology platform that supports the three personnel security missions, background investigations, continuous vetting, and adjudications in a one-stop-shop system for end-to-end personnel vetting called the National Background Investigation Services (NBIS). NBIS, which is being deployed incrementally as technical capability grows, will modernize technology capabilities leveraged by DCSA and is a critical to implementing Trusted Workforce 2.0.

This state of the art system will unify where mission areas and other functions across DCSA and the government will perform their work and share information to protect national security and manage the Trusted Workforce.

NBIS integrates improved cyber security capabilities, maximizes process and technology efficiencies, and enables agencies, through shared services, to quickly adapt to policy and operational changes through system configuration while continuously improve the quality and timeliness of its products and services.

Ongoing NBIS transitions, mainly moving current and potential civilians, military, and contractors working on behalf of the federal government to eApplication (eApp), greatly improves user experiences and integrates enhanced technology capabilities to decrease process timeliness.

A feat of this magnitude requires that mission areas from across the agency work hand in hand with the Program Executive Office/NBIS to tailor capabilities and features to meet the needs of many different end users including investigators, adjudicators, analysts, external customers, and applicants.

Leslie Reid, Senior Technical Advisor for Personnel Security, noted that NBIS is not being developed in a vacuum. Subject matter experts from across mission areas at DCSA partner daily with the NBIS team and the group of internal and external stakeholders continues to expand as the systems capabilities come online.

"It is a partnership between the missions and the NBIS Program Office as we determine the requirements, develop, and test them together," Reid said. "Agile development allows for pivots and incremental delivery giving us time to learn and acclimate to the new technology before it becomes operational. The partnership and constant communication ensures the technology development meets the needs of the mission."

NBIS users are gradually operationalizing multiple capabilities like the position designation tool (PDT), case initiation/Electronic Application (eApp), adjudication technology, continuous vetting, and subject management. Enhancements to all elements of the system will continue to accommodate user needs and policy changes. Many other technical deliveries including background investigations functionality are in process. Operational planning efforts are in progress as the system matures.

In early February 2023, more than 80 people comprised of NBIS staff, developers, and Personnel Security leaders came together in Hanover, Md., for a Personnel Security and NBIS offsite which played a key role in strengthening the partnership and informing the ongoing development of NBIS. Sarah Souza, NBIS Planning & Deployment Office Lead for DCSA, says the event initiated the foundation of a great working relationship.

"This was really the first time that PS and NBIS were physically all together, in the same location. It was so great to see familiar faces and be introduced to new ones," said Souza. "Having everyone in person at Milestone presented opportunities for meaningful engagement, organic collaboration, and momentum for moving forward together."

Interactive demos helped attendees understand that increased visibility to each other's work will increase collaboration that will be in line with Trusted Workforce policy changes ultimately making for better products and information sharing. NBIS will empower users to manage their mission areas, and interchangeable components across multiple mission sets will reduce costs and improve interoperability.

Reid says breakout sessions during interactive demos allowed for each respective mission to dig deep into their own ongoing development equities with the technical team responsible for coding the system.

"The groups worked together to learn how to effectively test capabilities they designed together as they are developed. As the system becomes more mature, the testing becomes more complex and the Personnel Security end users are responsible for ensuring the code meets their requirements," Reid said. "This is a repeatable process that allows teams to learn from each other and collaborate, and that guarantees the best possible product."

During breakout sessions each mission spent time one-on-one with their NBIS planning and deployment point of contact where they worked on the strategy and process to operationalize the system. They discussed ideas for onboarding the workforce, the best way to define success, ongoing plans, and dependencies.

Operationalization dependencies discussed include not only technical dependencies but also non-technical factors such as data migration, customer preparation, and workforce training.

Also paramount to the conversation during the breakout sessions was the topic of how to cultivate workforce engagement. Over the course of the two days groups provided ideas and thoughts on process improvement. Feedback was consolidated into areas pertinent to growth and development between NBIS and the mission areas to include communications, roles and responsibilities, continuity of operations, data, and testing. As a result of the sessions, Reid and colleagues paired up staff from Personnel Security and NBIS to collaborate on 14 process improvement projects which have been briefed to the Deputy Director.

"The potential of this collaborative, organically driven, working group is endless," Reid said. "I look forward to our current projects coming to fruition as well as future ideas born out of this partnership."

Personnel vetting is on the cusp of a huge technology change with NBIS, along with monumental policy change brought by Trusted Workforce 2.0.

Partners recognize the complexity of this effort and each other's vastly different areas of subject matter expertise. Mark Pekrul, Deputy Assistant Director of Customer and Stakeholder Engagement at DCSA, says collaboration, commitment and partnership is crucial for success.

"NBIS is the single biggest sea-change, from an IT perspective, which has occurred since vetting systems were initially automated more than 35 years ago. We cannot succeed without commitment from all mission stakeholders, both technical and not, to continued, intensive collaboration and teamwork," Pekrul said. "This moment in time sees the greatest level of partnership yet in this endeavor, and it is this partnership which puts us in a place where we can most clearly see a path to success."

The initial reaction to change is often to resist it, especially when it requires the level of effort and commitment it takes to successfully produce and deploy a system like NBIS. However, the transition to NBIS will reinforce and fine tune the agency's commitment to national security, as the system will enable DCSA to seamlessly adopt and implement Trusted Workforce as well as adjust to future unknown personnel vetting changes as they arise.

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.



Scott Stallsmith is the Senior Procurement Executive (SPE) and the Senior Services Manager (SSM)

Scott Stallsmith is the Senior Procurement Executive (SPE) and Senior Services Manager (SSM), Contracting and Procurement Office. In this capacity he is responsible for interpreting and implementing higher level policies and regulations that directly shape and improve DCSA operations and customer interaction throughout the agency. He oversees a contract portfolio of over \$5 billion and is responsible for management direction of the acquisition system of the agency, including implementation of the unique acquisition policies, regulations, and standards.

Prior to his current role, Stallsmith served as a Contracting Officer supporting multiple agencies within the Intelligence Community for over 20 years. While at the National Geospatial-Intelligence Agency, he served as the lead Contracting Officer responsible for its multi-billion dollar information technology (IT) acquisition strategy that encompassed all infrastructure IT services. Additionally, he served as the senior Contracting Officer in a joint duty assignment to the Office of Director of National Intelligence. In this role, he was responsible for establishing the acquisition and contracting strategy for the Intelligence Community Information Technology Enterprise/Desktop Environment supporting 17 intelligence community agencies.

He obtained a bachelor degree in Business Administration from Roanoke College; a Master of Arts in International Commerce and Policy from George Mason University; and a Master of Science in System Engineering from George Washington University. Stallsmith is also a member of the Defense Acquisition Corps.





QUESTIONS AND ANSWERS

Q. We have your biography, but what is something that people should know about you? What brought you to DCSA?

I was a contracting officer, who had been working in the Intelligence Community (IC) for more than 20 years, and decided I needed a bit of a change. I wanted to broaden my understanding of federal contracts outside the IC realm. DCSA was a relatively new agency with a great mission, and it would need to establish a contracting office, which peaked my interest. The Head of the Contracting Activity (HCA) opened up, so I applied. As the Director was hiring me, he said the current Senior Procurement Executive (SPE) is about to leave and he wanted me to fill that role as well. So I applied for one job and got two. For the first three to six months, I was having to do both roles until I was able to hire my deputy, Clay Socha..

Q. Acquisition recently changed its name to Contracting and Procurement Office (CPO). What was the impetus behind that change?

The new name, Contracting and Procurement Office (CPO), more accurately encompasses the office's contribution to the full acquisition lifecycle. When referred to as "Acquisition," there is a larger process involved. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract. While CPO is responsible and involved in parts of this larger process, it takes a large team across DCSA to complete the entire process.

Q. What would you like readers to know about CPO?

CPO is in a year of growth. We have nearly doubled our staff in a few short months. With growth comes new ideas. Within our staff, we have diverse backgrounds from DCSA legacy organizations and from all across the federal government. That varied experience is providing robust conversations on best practices and improvements that CPO can implement. We are excited for the future of our office and services we will be able to provide DCSA.

Q. The Component Acquisition Executive (CAE) and CPO are establishing the Acquisition Center of Excellence. What is the goal of the ACE? Does establishment of the ACE fall in line with other DOD agencies?

The ACE was established to fulfill the requirements of the Services Acquisition Reform Act, which among other things, required the creation of an acquisition workforce training program. The ACE was implemented through DOD Directive and DOD Instruction issuances, and to serve as a centralized collaboration and tool repository hub to improve effective, efficient, and innovative Acquisition outcomes across the enterprise. The ACE is a collaborative effort co-chaired by the CAE and Senior Procurement Executive; however, many other DCSA offices are involved, such as CPO, Office of the Chief Financial Officer, Office of Small Business Program and Industry Engagement, Office of General Counsel, and Program Executive Office.

The ACE will facilitate customer and stakeholder engagement, support proven, repeatable processes, procedures, and tools for incorporation in agency operations and decision documentation, and provide continuous learning opportunities for the workforce. The goal is to develop a community of practice, and we've joined forces with the Component Acquisition Executive Office. We'll be holding events such as brown bags and conferences, where we'll discuss our growth and what it means to do acquisition and contracting at DCSA.

Q. Besides the ACE, what other initiatives is CPO considering for the future?

CPO is working on several programs and processes and the following are a few highlights. We are leading the effort to develop the DCSA Acquisition Workforce model and Guide Book, standing up the DCSA Government Purchase Card (GPC) Program, formalizing the inter/intra-agency (IAA) agreements (IAA) process and identifying improvements, and establishing a DCSA Grants Program.

In regards to that last item, the agency needs to request grant authority, it doesn't automatically come as part of the stand-up of an agency. As the agency ingests new missions, some of these missions have historically provided grants, such as the National Center for Credibility Assessment. A grant is an opportunity for the agency to put money for a public good. Sometimes good ideas might not get funded by the private sector, so grants are a way for the government to spark good ideas

Q. What are some of the challenges that CPO is currently facing? How are you tackling those challenges?

Since the formation of DCSA, CPO has struggled with staffing our office to the level needed to support the mission. When the agency was formed in 2019, we had a total staff of 64 employees, and in late April, that number had grown to 106. We are in the midst of several hiring actions, which are expected to bring our total workforce to 132, which is fully staffed with our current footprint (129 civilians and 3 reservists). As a relatively new agency, we have faced challenges including a need to draft policies and procedures to manage contracting actions, educate mission partners on the services we provide, and educate the DCSA acquisition workforce regarding the responsibilities associated with acquisition management within the DOD. I am happy to report progress on all fronts. Our Policy & Oversight office has been busy drafting a myriad of policies and helpful tools for DCSA. In addition, CPO has been working with mission owners to best align the required agency needs to the proper contract or interagency agreement. In fact, on March 21, 2022, CPO established the Service Acquisition Manager Office to govern all service agreements within the agency. Lastly, CPO has collaborated with the Component Acquisition Executive Office to continue to define the roles and responsibilities of the agency acquisition workforce for DCSA. This includes ensuring contract requirements are evaluated through proper governance process, validation of proper billet coding, identifying and providing sufficient training, and ensuring proper contract oversight is happening at all levels.



Large, faint, stylized letters Q, &, and A in the background.

DCSA recognizes the best in industrial security; 19 facilities receive Cogswell Awards in 2023

On June 7, 2023, the Defense Counterintelligence and Security Agency presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 19 cleared contractor facilities, during the annual NCMS training seminar in New Orleans, La. The Cogswell awards represent the “best of the best,” and the winning facilities’ security programs stand as models for others to emulate. These 19 facilities represent less than one-tenth of one percent of the approximately 12,500 cleared facilities in the National Industrial Security Program (NISP).

“The industrial security threat we face is a pressing national security challenge of today but it is a long term proposition — the work we do or fail to do now will have impacts

for years into the future,” said DCSA Deputy Director Daniel Lecce during remarks before the Cogswell ceremony. “DCSA’s role has to be to continue working with you, continuing our current efforts in support of your industrial security program requirements, and expanding our efforts everywhere possible.”

To qualify, for the Cogswell companies must establish and maintain a security program that exceeds basic National Industrial Security Program requirements. Recipients also help other cleared facilities establish security-related best practices while maintaining the highest security standards for their own facility.

The Cogswell Award selection process is rigorous. A DCSA industrial security representative may only

nominate facilities that have at a minimum two consecutive superior industrial security review ratings and which show a sustained degree of excellence and innovation in their overall security program management, implementation and oversight. DCSA makes the final selections.

Established in 1966, the award honors Air Force Col. James S. Cogswell, the first chief of industrial security within the Department of Defense. Cogswell developed the basic principles of the Industrial Security Program, which includes emphasizing the partnership between industry and government to protect classified information. This partnership provides the greatest protection for U.S. warfighters and our Nation’s classified information.

Congratulations to the 2023 Cogswell Award Winners!

BAE Systems Land & Armaments L.P.
San Jose, Calif.

BAE Systems Land & Armaments L.P.
York, Pa.

Charles River Analytics, Inc.
Cambridge, Mass.

DCS Corporation
Alexandria, Va.

General Dynamics Information Technology, Inc.
Cherry Hill, N.J.

General Electric Company – GE Edison Works
Cincinnati, Ohio

Georgia Institute of Technology Georgia Tech Research Warner Robins, Georgia Field Office
Atlanta, Ga.

Infinity Systems Engineering, LLC
Colorado Springs, Colo.

Inmarsat Government, Inc.
Reston, Va.

KRI at Northeastern University, LLC
Burlington, Mass.

L3Harris NexGen Communications, LLC
Nashua, N.H.

Leonardo DRS
Bridgeton, Mo.

LexisNexis Special Services, Inc.
Washington, D.C.

Lockheed Martin Corporation – Lockheed Martin Aeronautics
Ft. Worth, Texas

Lockheed Martin Corporation – Sikorsky
Stratford, Conn.

National Institute of Aerospace Associates
Hampton, Va.

Northrop Grumman Systems, Corp.
St. Augustine, Fla.

SciTec, Inc.
Princeton, N.J.

The Texas A&M University System
College Station, Texas



DCSA Security Programs chief presented with Distinguished Presidential Rank Award

By John Joyce

Office of Communications and Congressional Affairs

Defense Counterintelligence and Security Agency Security Programs Office Chief Edward Fish Sr., a recipient of the Distinguished Defense Intelligence Executive Presidential Rank Award for fiscal year 2022, was recognized for his accomplishments at DCSA's first honor awards ceremony held in March 2023.

Fish, a previous recipient of the Meritorious Executive Presidential Rank Award, credited DCSA employees and leadership for their role in making the agency's phased transfer and transition an ongoing success since its establishment on Oct. 1, 2019.

"Everyone stepped up throughout our transformation and I couldn't have had a better security team," said Fish. "It was an honor to work closely with my team of professionals while serving in the front office and getting to better know Director Lietzau, the newly arrived Deputy Director Lecce, and all who followed. I was fortunate to have been given incredible support from the staff. In particular, I am deeply grateful for the support provided to me by front office personnel such as Ms. Paula Henry, Ms. Heidi Sikorski, Ms. Amanda Smith, and Ms. Adrianna D'Baron. I was further honored by working closely with true professionals such as Mr. Larry Vincent and Ms. Anita Galle. Additionally, I couldn't have had a better deputy chief of Security Programs in Lisa Gearhart who stepped into the breach as acting chief of Security Programs for almost a year while I served as acting DCSA chief of staff."

The award's justification statement points out that Fish continually advances the safety and security of the DCSA workforce by developing and executing effective agency-wide programs and training to foster a workforce-wide culture of awareness and vigilance.

"Throughout the mission, organizational, and environmental challenges of the past three years, Mr.

Fish maintained a keen focus on leader development," according to the justification statement.

"He ensures a diverse and inclusive workplace, engaging and leveraging collaboration and team effort to bring

out the best in his workforce, his leadership team, and his senior peers," the statement continued.

The Civil Service Reform Act of 1978 established the Presidential Rank Awards Program to recognize a select group of career members of the Senior Executive Service (SES) for exceptional performance over an extended period of time.

The justification statement cited specifics about Fish's executive leadership as follows:

"As the driving force of DCSA's response to the COVID-19 pandemic, Mr. Fish shaped a program that continues to ensure mission accomplishment and protection of the workforce. Since the onset of the pandemic in early 2020, the DCSA workforce has consistently maintained positive COVID-19 case rates that were 75% less than the trending U.S. case rates. Our low case rates, as compared to the rest of the country writ large, are largely due to Mr. Fish's engaged leadership and his enduring efforts that stressed collaborative planning, timely communication, strict adherence to established force health protection measures, and sustainment of a robust telework program.

"As Chief of the DCSA Security Programs Office, he merged and transformed legacy and new assets into a coherent team to address security, insider threat, and mission assurance challenges of DCSA's nearly 10,000 affiliated personnel operating at 167 locations across the country. He led efforts to assess and improve security of all DCSA offices, establishing standard requirements for vetting DCSA affiliates, anti-terrorism and force protection, emergency management procedures, actions for clearance access suspension, and guard force operations."



DCSA Director William Lietzau (left) presents Edward Fish, chief of Security Programs, with a DCSA Director's coin during an agency awards ceremony in March. (DOD photo by Christopher P. Gillis)

'Integrate' tabletop exercise focuses on gaps in information sharing, proposes solutions

By Beth Alber

Office of Communications and Congressional Affairs

As part of the Unity of Effort enterprise goal in the Defense Counterintelligence and Security Agency Strategic Plan 2022-2027, DCSA is working to step away from its legacy silos to build an integrated agency that leverages its combined expertise to accomplish national security missions. A big part of achieving that effort is communication. To improve on these processes, the agency gathered employees from all mission areas, with a blend of headquarters and field representatives, to discuss the value of an Information Sharing Handbook built specifically for the event, and identify gaps and process improvement solutions to improve information sharing.

Over a two-day period, 45 agency employees participated in a "Integrate" Tabletop Exercise (TTX) hosted by the Chief Strategy Office (CSO) that involved working through a scenario-based simulation and holding collaborative discussions focused on identifying achievable actions. The event also focused on advancing the "Gatekeeper" culture initiative, with the goal of participants gaining a new understanding of other mission areas, cultivating networking opportunities, and increasing trust in other teams.

The "Integrate" TTX centered on a hypothetical scenario of industrial espionage by a foreign adversary, in which teams from Counterintelligence and Insider Threat, Industrial Security, and Personnel Security had to determine what information needed to be shared, whether the information was valid, and how best to share the information.

Each mission area was housed separately while working through the scenario. At the end of the event, participants shared feedback about struggles with sharing information when not knowing the level of access of their counterparts; and the constant need to triage information and validate its usefulness. Additionally, participants gave feedback on the handbook, recommending it be incorporated into future training and policy guidance.

On day two, attendees participated in facilitated discussions using a gallery walk, which involved exploring multiple texts or images placed around the room. This provided attendees the opportunity to give feedback on perceived information sharing gaps related to eight categories

(technology, personnel, culture, policy, organization, facilities, processes, and training) eventually identifying over 40 common issue areas and gaps, and recommending more than 35 possible solutions. Participants then voted to prioritize one solution from each of the categories to focus on in the near future. One priority solution recommended offering information sharing TTXs at the regional offices, as personnel want more hands-on training. Another proposed solution emphasized the need for DCSA leadership to communicate and model information sharing, to develop a culture that empowers the workforce. Within the policy category, the proposed solution was to create a policy library that houses all current policies across mission sets. The recent creation of the Enterprise Policy Program (EPP) within the CSO is the first step in accomplishing this solution. The EPP transitions the agency from a disparate policy execution program to a unified, synchronized, and integrated formal DCSA regulatory program and structure.

"The TTX started the conversation necessary to identify barriers, challenges and critical changes needed not only in our way of thinking and the way we communicate, but the necessary changes we need to make in our policies and procedures," said Christy Morris, Keesler Air Force Base Resident Office, Field Operations. "We will not meet the mission if we continue to operate in a vacuum within our own silos. We must leverage the strengths of one another, and we must reach across the proverbial table."

While the "Integrate" TTX was just one step toward the agency achieving its vision, the results of the exercise have already started filtering into the day-to-day operations of the mission.

"In the weeks following the TTX, I have found multiple opportunities across DCSA that promoted information sharing that wouldn't have happened without it," said Andrew Parker, National Access Elsewhere Security Oversight Center, Industrial Security. "Both the information sharing concept and how it was presented at the TTX seem to have been a catalyst among the directorates at the operational level in sharing both information and how we can use it better to support DCSA's mission."

Enterprise Governance Framework supports efficient decision-making for agency

How does DCSA make decisions and manage its initiatives in alignment with the Agency's mission and goals?

Through the Enterprise Governance Framework, which supports efficient and effective decision-making. DCSA is a transformative agency that incorporates values and practices from both its DOD and corporate partners. As America's Gatekeeper, it is important for DCSA to have a rigorous system in place to achieve the mission and enterprise goals outlined in the strategic plan.

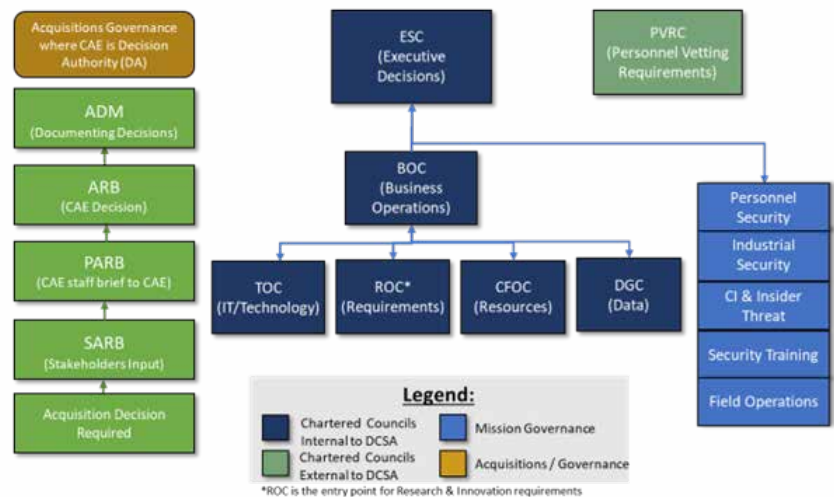
DCSA's legacy governance flow and structure was no longer best serving the organization, so DCSA formally updated its enterprise governance model in June 2022. DCSA's renewed governance structure aims to cover all key functions, establish clear reporting, and allow governance bodies to have authority to oversee their functional area as needed. Six councils were established to facilitate governance operations at DCSA. The Chief Strategy Office (CSO) is responsible for oversight and serves as the Executive Secretariat for DCSA enterprise-level governance operations.

The governance structure follows a tiered model, with the Executive Steering Council (ESC) serving as the top-tier oversight body. The ESC is the senior leadership forum that establishes strategic goals, oversees initiative implementation, and makes decisions that impact the entire enterprise. Chaired by the director of DCSA, the ESC ensures that senior leadership has insight into agency-wide strategic goals and operations.

The Business Operations Council (BOC) serves as a mid-tier oversight body for several key functional areas. The BOC replaced the legacy Corporate Integration Council and oversees day-to-day business operations.

The next tier of councils includes the Technology Oversight Council (TOC), Requirements Oversight Council (ROC), Chief Financial Officer Council (CFOC), and Data Governance Council (DGC). The TOC is responsible for overseeing technology policy, infrastructure, and security. The ROC collects, analyzes, validates, and prioritizes DCSA requirements prior to acquisition governance. The CFOC oversees financial planning and decisions. The DGC oversees data, information, and analytics policy.

Acquisition oversight responsibilities of the Component Acquisition Executive (CAE) are executed in accordance with applicable DoD policies and instructions. The CAE's primary functions include overseeing cost, schedule, and performance for acquisitions not delegated to a subordinate decision authority (DA). The Acquisition Review Board (ARB) is the principal forum for making acquisition decisions. Prior to an ARB, the CAE staff will conduct a Stakeholder's Acquisition Review Board (SARB) to ensure all stakeholders are aware of and have a voice in the acquisition process.



Over the course of the past year, much work has been done to ensure collaboration, develop issue-escalation or referral thresholds, and outcome-focused decision-making forums. Emphasis has been placed on the creation of the DCSA requirements and acquisition processes through the establishment of the ROC and accompanying acquisition governance bodies.

The established governance councils promote participation by leaders and staff at all levels. Mission areas across the agency are represented through membership in the various councils. Members are encouraged to communicate with DCSA employees within their mission area and to elevate issues/matters for discussion when needed. Representation of each member's own mission area is an underlying factor related to the success and effectiveness of DCSA's governance forums. DCSA employees at all levels should communicate matters up the ladder to their mission leaders.

To maintain SPeD certifications, acquire required Professional Development Units

The Security Professional Education Development (SPeD) Certification Program is part of the Department of Defense's (DOD) initiative to professionalize the security workforce. This initiative is for individuals performing security functions on behalf of DOD and ensures a common set of competencies exist among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals. The SPeD Certification Program is codified as a requirement for those individuals performing security functions on behalf of the DOD in DOD Instruction 3305.13, "DOD Security Education, Training, and Certification" and DOD Manual 3305.13, "DOD Security Accreditation and Certification."

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

Each program has its own set of eligibility and prerequisite requirements that candidates must meet prior to testing. For example, the Antiterrorism Credential (ATC) is only for individuals currently serving in antiterrorism officer (ATO) positions. After meeting the eligibility and prerequisite requirements, candidates must attempt the test in a secure, proctored environment at one of the program's network of testing centers. Candidates who pass the test and meet all other requirements are conferred for a period of two years.

During these two years (also known as the certification maintenance period), candidates are required to successfully complete at least 100 Professional Development Units (PDUs). There are various to acquire these PDUs:

PDU Category 1: New Certification or Credential	PDU Category 4: Security Conferences
1A: New SPeD or Adjudicator Professional Credential (APC) Certification: Each New SPeD or APC Certification is valued at 100 PDUs.	4A: Security Conference: Participant: Each Hour of Security Conference as a Participant is worth 1 PDU.
1B: SPeD Credential or the Due Process Adjudicator Professional Credential (DPAPC): Each SPeD Credential or the DPAPC is valued at 75 PDUs.	4B: Security Conference: Presenter: Each presentation is worth 5 PDUs, with a max of 25 per event (total of 5 presentations)
1C: Non SPeD or APC Certification: Each Non-SPeD Certification is valued at 50 PDUs.	
PDU Category 2: Security-Related Training	PDU Category 5: Security-Related Projects
2A: Security Related eLearning Course: Each Hour of Security-Related eLearning Course earns 1 PDU (partial hours round up).	5A: SPeD Certification Projects: Certificants can receive three PDUs per contact hour and two PDUs per completed homework assignment for a distinct project.
2B: Security Related Instructor-Led Training (ILT) or Virtual Instructor-led Training (VILT) Courses	5B: Non SPeD Certification Projects: Certificants can receive three PDUs per contact hour and two PDUs per completed homework assignment for a distinct project.
2C: Security Related Higher Education: Each WEEK of Security Higher Education earns 10 PDUs.	
PDU Category 3: Non-Security Related Training	PDU Category 6: Other Professionalization
3A: Non-Security Related eLearning Training Courses: Each Hour of Non-Security-Related eLearning Training Courses earns 1 PDU (partial hours round up).	6A: Other Voluntary Professionalization Activities: Certificants can received 2 PDUs per contact hour.
3B: Non-Security Related ILT or VILT Courses: Each FULL DAY of Non-Security Related ILT or VILT Courses earns 10 PDUs.	
3C: Non-Security Related Higher Education: Each WEEK of Non-Security Higher Education earns 10 PDUs.	
Full version of the PDU Fact Sheet can be downloaded at: https://www.cdse.edu/Portals/124/Documents/certification/pdu-category-fact-sheet.pdf .	

DCSA employees, teams honored at Director's Awards and Recognition Program Ceremony

By John Joyce

Office of Communications and Congressional Affairs

Defense Counterintelligence and Security Agency (DCSA) employees and teams were recognized for their contributions that positively impacted national security during the agency's first awards ceremony.

The annual DARP awards for fiscal year 2022 honored the DCSA Junior Employee of the Year, Employee of the Year, Senior Employee of the Year and Service Member of the Year. In addition, the director's program honored the DCSA Team of the Year and another DCSA team for Excellence in Innovation during the March 2023 event held at the agency's headquarters in Quantico, Va.

The Senior Employee of the Year Award was presented to Amber Jackson, curriculum manager in the Insider Threat Division at the Center for Development of Security Excellence.

As cited in the award nomination, "Ms. Jackson significantly contributed to educating Federal and Industry professionals on insider threat topics by quickly responding to customer needs. She conducted a training needs analysis and worked with stakeholders, and successfully led the development of a Vigilance Video Series that addressed concerning behavior, reporting, critical thinking, risk, social media engagement, an Escape Room game, app content and case studies. She also helped plan, coordinate, and host the Virtual Insider Threat Conference, as well as a product awareness webinar. She expanded awareness of CDSE, insider threat training and resources through briefings, communications and social media. Ms. Jackson proficiently managed numerous products regarding insider threat including 12 e-Learning courses, 43 job aids, 19 security training videos, 9 security awareness games, toolkits, 27 webinars, and 44 case studies, a campaign website, a graduate course, and one mobile app."

"It is amazing to be recognized for my hard work and



DCSA Director William Lietzau (left) presents the Senior Employee of the Year award to Intelligence Operations Specialist Amber Jackson from the Center for Development of Security Excellence, during DCSA's first official Awards ceremony at the Russell-Knox Building headquarters, Quantico, Va., March 10, 2023. (DoD photos by Christopher P. Gillis, OCCA).

dedication. I am grateful to be selected amongst the many outstanding fellow gatekeepers at DCSA," said Jackson. "Do not be concerned with others' perception of you. You are qualified, your experience is legitimate, and you are a professional. You can be charismatic or introverted and find success; you can be a leader or remain in the background and still be industrious. Honestly, sometimes being annoying is what produces results, yet simply listening can also put you in the right position. Regardless, stay determined and committed to completing the mission."

The Employee of the Year Award was presented to Michael Benner, chief of staff (Security Programs Office).

The award nomination stated that Benner epitomized professionalism by spearheading the management of DCSA's Security Services Center's daily operations for in-processing procedures through fiscal year 2022. As part of the daily operations, Banner tracked badges and courier cards, issued IC badges for DCSA new hires,

completed visit requests for distinguished visitors and foreign delegations, and handled the issuance of common access cards for contractors in-processing in support of DCSA. "His performance was exceptional and was the driving force behind Security Services section's success in the management of an unprecedented 17,600+ security actions between the months of October 2021 and September 2022," the nomination stated. "Mr. Benner demonstrated exceptional professionalism by going above and beyond in assuming responsibilities as the lead Security representative for over 236 VIP visitors for the front office and provided outstanding customer service while supporting four high profile foreign delegation visits, ensuring each visit was coordinated in a timely manner, and visitors encountered no security delays or interruptions."

"I was excited and shocked upon finding out that I was recognized for this award," said Benner. "I am incredibly grateful for my colleagues and leadership who have supported the team that provides the agency support. Without that, I couldn't have been as successful and I personally want to thank the Security Services team for this accomplishment."

The Junior Employee of the Year Award was presented to Autumn Webster, Field Operations (Counterintelligence).

As noted in the award nomination, "Mrs. Webster's performance was simply amazing! Her efforts with the CI Awareness and Reporting (CIAR) briefing, Suspicious Contact Report (SCR) triaging, and Intelligence Information Report (IIR) writing processes significantly improved the final products for each of these efforts. The security reviews, where she assisted in the CIAR briefings, were well received and praised by each facility. She helped triage over 100 SCRs and was the primary author of 10 IIRs and drafted another 36 IIRs that were disseminated to the Intelligence Community. She helped ensure over 1,515 DCSA employees received a CIAR brief to meet



DCSA Director William Lietzau (left) presents the Employee of the Year award to Security Specialist Michael Benner from Security Programs.

their mandatory annual training requirement. Her preparation and engagement for the Region's All-Hands was outstanding. Participants and guest speakers were thoroughly impressed with the entire effort from the logistics to the content.

"I was happy to be given the opportunity to work at DCSA," said Webster, who is a CI Special Agent in the Mid-Atlantic Region. "Our mission and work is very important. When you truly believe in what you are doing, it will always impact your work positively. I was able to have a lot of success because of my colleagues — my office has a very positive attitude and immediately treated me like a team player. Sometimes the difference between having success or not is just whether you had the opportunity to show what you can do, I always feel like I was given opportunity since arriving at DCSA."

The Service Member of the Year Award was presented to Army Master Sergeant Vida Kwarteng, Personnel Security (Background Investigations).

The award nomination's impact statement described

Kwarteng as demonstrating dependability with every program or activity that she supported. "Kwarteng's contributions helped increase the number of Background Investigations employees recognized for special act and service awards by almost 300%, ensuring BI had Director's Award and Recognition Program representation each quarter. She was also instrumental in the Customer and Stakeholder Engagement fiscal year 2022 budget being accurately executed and the fiscal year 2023 spend plan being submitted on time. The executive secretary team also benefited from her consistent professionalism, dedication to quality, and willingness to learn and pitch in no matter the task. Her overall impact extended past the executive secretary as each employee reaped the benefits of her efforts."

"When you work for a great organization, and receive great leadership and direction from someone like Dr. Robin Young, Background Investigations chief of staff, it inspires you to work hard and to only do your very best," said Kwarteng. "I work alongside some really great people, to include Anjanette Crall, the supervisory program specialist for the Background Investigations executive secretary team, whose training and encouragement allowed me to quickly find where I could be most helpful. I appreciate the recognition, but I am most proud of knowing that I contributed to Background Investigations, and ultimately the DCSA mission, in a significant way."

The Team of the Year Award was presented to DCSA's National Name Check Program — Continuous Vetting Pilot Team (NNCP).

"Overall, the NNCP Continuous Vetting Pilot project team successfully established and demonstrated a vital new capability for the U.S. government that will directly enable federal personnel vetting reform under Trusted Workforce," said Ryan Dennis, NNCP Continuous Vetting Pilot project team lead. "In addition to identifying and taking personnel security risk mitigation actions on numerous subjects during the pilot, the team delivered major improvements in NNCP timeliness, quality, utility and business



DCSA Director William Lietzau (left) presents the Junior Employee of the Year award to Intelligence Operations Specialist Autumn Webster from Counterintelligence Field Operations Mid-Atlantic region.

rules. The partnership between the FBI Enterprise Vetting Center and DCSA was the epitome of inter-agency partnership. I am proud to have had the opportunity to be involved in this project and I am excited for the NNCP Continuous Vetting product to be available to the federal enterprise."

Members of the team included from Vetting Risk Operations: Jennifer Jo Powell, Robert Miller, Britni Ahlquist and Michael Stedman; from Background Investigations: Janeen Beatty and Melanie Hilliard; from Program Executive Office: Sarah Souza; from Counterintelligence



DCSA Director William Lietzau (fourth from left) presents the Team of the Year award to Personnel Security Vetting Risk Operations team for their efforts related to a National Name Check Program (NNCP) Continuous Vetting (CV) pilot.

and Insider Threat: Sara Kramer; and from the Office of General Counsel: James Clark.

The Excellence in Innovation of the Year Award was presented to the Risk Evaluation Innovation Team. Members of the team included Michael Sibley and Anastasia Baker from the National Access Elsewhere Security Oversight Center (NAESOC) in Industrial Security.

As outlined in the award nomination, at the beginning of fiscal year 2022, the NAESOC Team and the regional mission directors realized that it was neither efficient nor appropriate for security reviews to be conducted remotely at the NAESOC. So the NAESOC team created the Risk Evaluation (RE) Process in order to assess risk at the large number of facilities in the NAESOC using government and contractor employees and within a shorter period of time. This process “allows all NAESOC facilities to be contacted every 2.5 years, with a process that incorporates the use of open source information, DCSA internal databases, and contractor assistance to supplement the government ISRs (industrial security representatives) in the NAESOC. It already has yielded 398% more vulnerabilities and 30 times more risk stories on 10 times more facilities than the original processes.”

In a joint statement, NAESOC Branch Chiefs Ana Baker and Mike Sibley reacted to the award. “NAESOC was stood up to enhance the risk identification process used for access-elsewhere facilities,” they said. “Through our risk evaluation process we are assessing and mitigating risk at an unprecedented rate of return. This success is a result of our teams’ critical thinking and commitment to innovation within industrial security oversight. We are thrilled the impact was recognized by Industrial Security and DCSA, at large.”



DCSA Director William Lietzau (left) presents the Excellence in Innovation of the Year award to the National Access Elsewhere Security Oversight Center (NAESOC) Risk Evaluation Team members Senior Industrial Security Specialists' Michael D. Sibley (right) and Anastasia A. Baker from the Industrial Security NISP Operations branch, during DCSA's first official Awards ceremony.

Recognizing 50 years of service, agency places wreath at Tomb of the Unknown Soldier

By John Joyce

Office of Communications and Congressional Affairs

DCSA leaders placed a wreath at the Tomb of the Unknown Soldier at Arlington National Cemetery in honor of the agency's 50th anniversary of support to national security during a May 1 ceremony.

Moreover, the official party — DCSA Director William Lietzau; Chief of Staff Ellen Ardrey; Employee of the year Mike Benner; and Jeffrey Flora, one of the longest serving members of the agency — honored leaders of DCSA predecessor organizations responsible for background investigations and industrial security at two more gravesites.

After placing the wreath at the Tomb, DCSA employees walked to the gravesite of Air Force Col. James Cogswell — the nation's first Director of the Unified Office of Industrial Security — who helped lay the foundations of the National Industrial Security Program. Lietzau and Ardrey placed flowers in front of the headstone.

"It's an honor to be here and recognize this (DCSA's 50th anniversary) for the whole agency. Not everyone in the cemetery died in combat," said Lietzau at the ceremony held at Cogswell's gravesite. "They all served in a significant way and in some ways, Col. Cogswell represents the perfect combination of those (who died in combat or otherwise).

He understood what happens when things don't go well in combat, but he also completely understood — as the first Chief of the Industrial Security office — what happens in-between those punctuation marks (between conflicts and wars) in our history is what really determines the future of this country."

The Cogswell Award — established in 1966 and presented annually to cleared facilities with exceptional security programs — is named for Cogswell and honors his emphasis on the true partnership between industry and government to ensure the protection of classified information, materials and programs.

DCSA employees held another ceremony at the gravesite of Air Force Brig. Gen. Joseph Cappucci, the first Director of the Defense Investigative Service (DIS), where DCSA Employee Council co-chair Andrea Brett and council member Allison Mayes placed flowers in front of the headstone.

"He brought Background Investigations (BI) into our mission set and consolidated among the military services that were doing BI at the time," said Lietzau at the gravesite ceremony. "If you think about what we did with the new name of DCSA — we consolidated it all for the whole U.S. government. I have no question that would have been absolutely consistent with Gen. Cappucci's vision."

In effect, DCSA is recognizing two anniversaries in fiscal year 2023 thanks to a Secretary of Defense memorandum issued more than 50 years ago.



A member of the U.S. Army's 3rd Infantry Regiment, "The Old Guard," puts the wreath for the DCSA 50th Anniversary Wreath Laying into place, followed closely by a bugler with the U.S. Army "Pershing's Own" band. (DOD photo by Cindy McGovern, OCCA)

The memorandum signed by Secretary of Defense Melvin Laird established the Defense Investigative Service, which became operational on Oct. 1, 1972. DOD Directive 5105.42 designated DIS as a separate operating agency under the direction of the Secretary of Defense.

That 1972 DOD directive — authorizing a workforce of 1,750 military personnel and 1,250 government civilians to conduct all DOD personnel security investigations — has retained its unbroken authority over the course of 50 years as DIS was renamed the Defense Security Service in 1999 and eventually consolidated with other organizations and renamed DCSA in 2019.

Hence, the agency celebrates 50 years of service while recognizing that DCSA achieved its third anniversary in October of 2022.

After a half century, the agency not only retains the same charter in its evolution from DIS to DSS to DCSA, it is still responsible to the nation as its Gatekeeper for personnel security and vetting.

The founding DOD directive, also known as the “Charter for the Defense Investigative Service,” defined the DIS mission: “To provide DOD components and other U.S. government activities, when authorized by the Secretary of Defense, with a single centrally directed personnel security investigative service.”

Similar to today’s DCSA personnel security mission encompassing security clearance investigations for military, government and cleared industry, DIS performed routine security clearance investigations for defense contractor personnel, as overseen by the Defense Industrial Security Clearance Office.

“It’s significant to recognize our past and recognize that we’re doing in many ways what’s represented here in this cemetery,” said Lietzau as the last ceremony concluded at Cappucci’s gravesite.



With the assistance of the U.S. Army's Old Guard, DCSA Director William Lietzau and DCSA Chief of Staff Ellen Ardrey place a wreath at the Tomb of the Unknown Soldier at Arlington National Cemetery in honor of the agency's 50th anniversary during a May 1 ceremony. In the back row are Employee of the Year Michael Benner, DCSA Security Office, and Jeffrey Flora, Deputy Assistant Director for Quality, one of the longest serving employees in the agency. (DOD photo by Quinetta Budd, OCCA)



DCSA Employee Council co-chair Andrea Brett (left), Chief Strategy Office, and council member Allison Mayes, Vetting Risk Operations, place flowers in front of the headstone of Brig. Gen. Joseph Cappucci, first director of the Defense Investigative Service.



DCSA Director William Lietzau and DCSA Chief of Staff Ellen Ardrey place flowers at the gravesite of Col. James S. Cogswell, for whom the James S. Cogswell Outstanding Industrial Security Achievement Award is named for.

NCCA unveils collaborative multi-disciplinary lab capability to impact national security

An unveiling of the new National Center for Credibility Assessment (NCCA) Research Collaboration Center revealed its innovative academic and scientific capabilities designed to foster collaborative solutions impacting national security during a tour and ceremony at Fort Jackson, S.C.

Defense Counterintelligence and Security Agency (DCSA) Director William Lietzau — among those touring the laboratory with NCCA and University of South Carolina leadership in late March — saw a research center where a cadre of scientists, engineers, and operational experts have already begun to apply scientific approaches addressing capability gaps of its federal partners.

“We’re developing a thoughtful research and development program,” said Lietzau as keynote speaker at the unveiling ceremony. “We’re working on a thoughtful way forward on how we’re going to assess the credibility of our workforce and assess our relationships with the academic community in general. This laboratory is absolutely key to what we accomplish moving forward.”

The multi-disciplinary nature of proposed solutions often requires NCCA to collaborate with outside specialists.

To address this ever-present need, NCCA pursued a collaborative relationship with the University of South Carolina, enabling access to substantial capabilities in critical academic and scientific areas of need for NCCA.

An essential component of this relationship was the establishment of the laboratory as a research collaboration center near the Columbia, S.C.-based university.

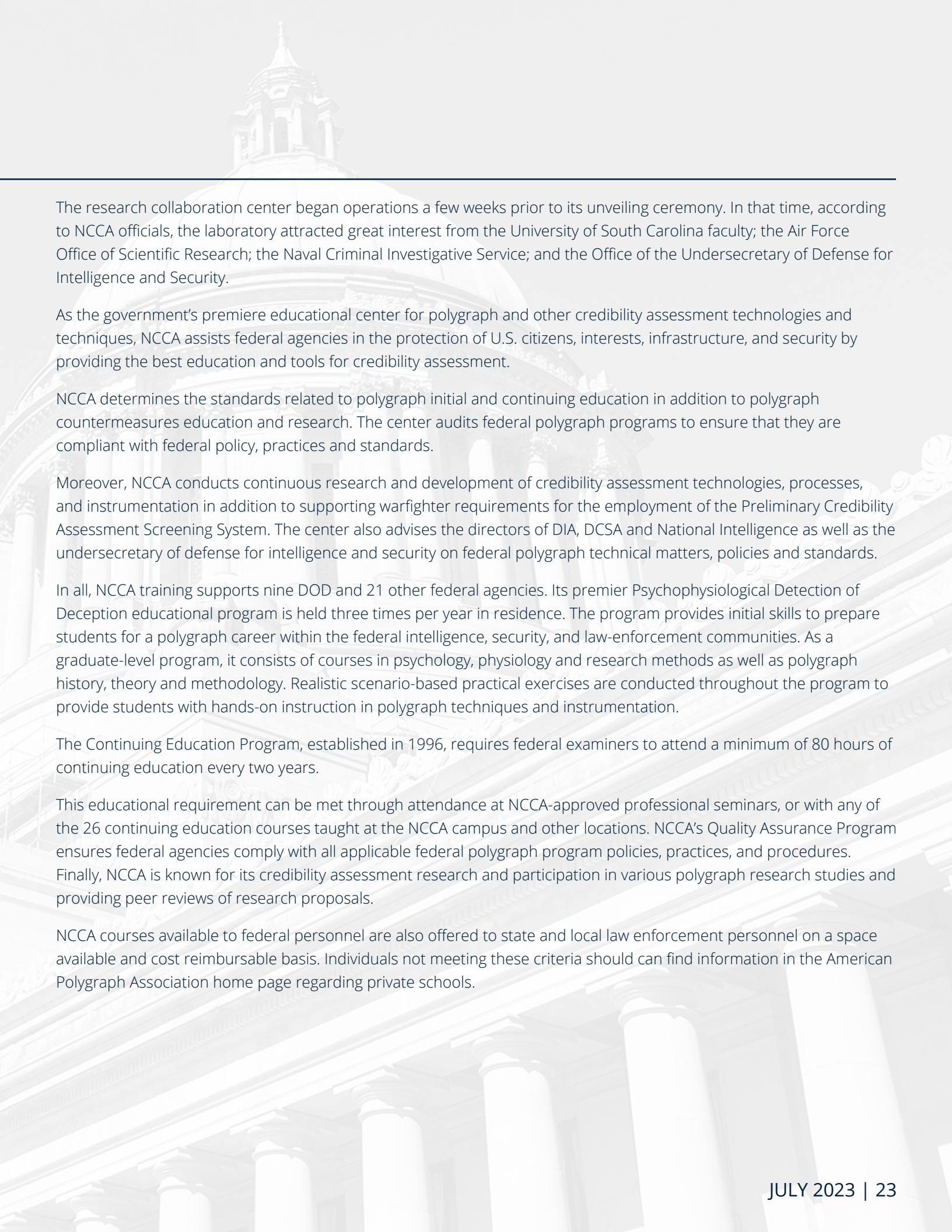
“We have to up our game and start imagining a way to accomplish our mission with better technologies, processes and policies than we currently have,” said Lietzau. “We need your support for that and that includes collaboration with universities that take security seriously.”

Specifically, the NCCA research collaboration center capabilities include:

- Multi-disciplinary expertise in engineering, computer science, physiology, behavior, linguistics, ethics, medicine, education and law.
- Undergraduate and graduate student researchers.
- Professional development opportunities for government scientists and engineers.
- Access to other research and funding opportunities.



DCSA Director William Lietzau speaks at the unveiling of the National Center for Credibility Assessment new research collaboration center. (DOD photo by Christopher P. Gillis).



The research collaboration center began operations a few weeks prior to its unveiling ceremony. In that time, according to NCCA officials, the laboratory attracted great interest from the University of South Carolina faculty; the Air Force Office of Scientific Research; the Naval Criminal Investigative Service; and the Office of the Undersecretary of Defense for Intelligence and Security.

As the government's premiere educational center for polygraph and other credibility assessment technologies and techniques, NCCA assists federal agencies in the protection of U.S. citizens, interests, infrastructure, and security by providing the best education and tools for credibility assessment.

NCCA determines the standards related to polygraph initial and continuing education in addition to polygraph countermeasures education and research. The center audits federal polygraph programs to ensure that they are compliant with federal policy, practices and standards.

Moreover, NCCA conducts continuous research and development of credibility assessment technologies, processes, and instrumentation in addition to supporting warfighter requirements for the employment of the Preliminary Credibility Assessment Screening System. The center also advises the directors of DIA, DCSA and National Intelligence as well as the undersecretary of defense for intelligence and security on federal polygraph technical matters, policies and standards.

In all, NCCA training supports nine DOD and 21 other federal agencies. Its premier Psychophysiological Detection of Deception educational program is held three times per year in residence. The program provides initial skills to prepare students for a polygraph career within the federal intelligence, security, and law-enforcement communities. As a graduate-level program, it consists of courses in psychology, physiology and research methods as well as polygraph history, theory and methodology. Realistic scenario-based practical exercises are conducted throughout the program to provide students with hands-on instruction in polygraph techniques and instrumentation.

The Continuing Education Program, established in 1996, requires federal examiners to attend a minimum of 80 hours of continuing education every two years.

This educational requirement can be met through attendance at NCCA-approved professional seminars, or with any of the 26 continuing education courses taught at the NCCA campus and other locations. NCCA's Quality Assurance Program ensures federal agencies comply with all applicable federal polygraph program policies, practices, and procedures. Finally, NCCA is known for its credibility assessment research and participation in various polygraph research studies and providing peer reviews of research proposals.

NCCA courses available to federal personnel are also offered to state and local law enforcement personnel on a space available and cost reimbursable basis. Individuals not meeting these criteria should can find information in the American Polygraph Association home page regarding private schools.



**Defense Counterintelligence
and Security Agency**

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil

571-305-6562

www.DCSA.mil