Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper

Volume 2, Issue 2

DCSA LEADERS SUPPORT BILATERAL EFFORTS WITH JAPANESE

IN THIS ISSUE

IN THIS ISSUE

Vol 2 | ISSUE 2

DCSA Gatekeeper

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

FROM THE DIRECTOR

As I contemplate the close of my second year as DCSA Director, I cannot help but reflect on the oath of office I took in an empty conference room after the workforce was sent home in response to COVID. Two years ago, few would have imagined that the workplace would still be impacted by the lingering effects of COVID today. Even fewer could have predicted DCSA's astounding mission success while not only contending with the impacts of COVID, but doing it during a period of significant transition. As we welcome the decline in infection rates and the gradual reentry to business and government offices, we can all be very proud of the work we have accomplished together.

This issue's article, "By the Numbers," highlights some of this success. The summary provides a clear picture, not only of the volume of work done in the past year, but also of the breadth and diversity of that work — from adjudicating clearances, to certifying and accrediting IT systems, to insider threat reporting. DCSA employees are well and faithfully delivering on our core missions in ways that surpass accomplishments of the past. Our employees prove every day that establishing DCSA as America's gatekeeper was the right thing to do for this nation's security.

While the metrics are impressive, we must remain focused on the future. The security threat is evolving every day, and DCSA is charged with keeping a step ahead of our adversaries. With that goal in mind, we developed the first DCSA five-year strategic plan to set the Agency's direction for the future. You can read more on the plan in these pages. Our 2022-2027 Strategic Plan aligns with broader intelligence and defense strategies and lays the foundation to accommodate DCSA's expanding missions while guiding our continued transformation efforts.

A concrete example of the Agency's transformation is illustrated in our cover story on DCSA support to the U.S.-Japan Bilateral Information Security Consultations (BISC). This integrated effort in support of our Japanese counterparts provided assistance in operations, policies, technologies, and data management. The holistic manner in which we engaged with our Japanese allies exemplifies how DCSA must work in the future to optimize mission performance. By breaking free from silos, we can better understand the security environment and improve performance across the spectrum of our mission sets. Another example of our organizational transformation is provided in the article on the Adjudications Directorate's work with the National Background Investigation Services (NBIS) team, transitioning adjudications from the Defense Information System for Security (DISS) to NBIS. The transition to NBIS will be challenging as we cannot use traditional acquisition methods. The security requirement for NBIS exists now, and we need to deploy the system as we develop it.

Finally, this issue's "Ask the Leadership" section introduces our new Deputy Director, Dan Lecce. With Dan, I am confident we have exactly the right person for this moment in DCSA's history. Dan is a tested leader with experience driving strategic change and posturing organizations to meet future challenges. He is also an executive with extensive experience managing personnel, financial, and information requirements — all critical issues for DCSA. Over the next few months, Dan and I will travel to meet with employees and stakeholders to hear firsthand how we can better support you.

Thank you for your continued support to DCSA as we execute our role as America's Gatekeepers.

William K. Lietzau
Director,
Defense Counterintelligence
and Security Agency

DCSA LEADERS SUPPORT BILATERAL EFFORTS WITH JAPANESE, MAKE IMPACT ON STANDARDIZATION OF INFORMATION SECURITY PRACTICES

By John J. Joyce
Office of Communications and Congressional Affairs

Defense Counterintelligence and Security Agency (DCSA) leaders – in support of their Japanese counterparts over the course of several years – are making a significant impact on bilateral efforts to standardize information security practices across the U.S.-Japan Alliance.

It began when the agency's senior experts — experienced in directing U.S. background investigations, vetting risk operations and adjudications — responded to a request from the Defense Technology Security Administration (DTSA) in 2019 to support the U.S.-Japan Bilateral Information Security Consultations (BISC). The BISC is a bilateral group committed to ensuring substantially equivalent information security practices between the U.S. and Japan — a key cooperative initiative to strengthen the Alliance.

U.S. Secretary of State Antony Blinken and Secretary of Defense Lloyd Austin discussed the importance of strengthening and reinforcing information security practices with Japan's Minister for Foreign Affairs Yoshimasa Hayashi and Minister of Defense Nobuo Kishi during the U.S.-Japan Security Consultative Committee held virtually in Washington, D.C. and Tokyo, Japan on Jan. 6 and 7, 2022.

"You can't measure the importance of this BISC effort," said Scott Nelson, deputy chief of DTSA's Regional Engagement Division, who contacted DCSA with his request for their expert assistance. "Information security is the basis on which all our collaboration to share information and technology will be built."

The BISC – formed as a result of a 2009 U.S.-Japan summit meeting between Prime Minister Yukio Hatoyama and President Barack Obama – launched a new process of consultations in order to strengthen security cooperation, including information security that deepens the U.S.-Japan Alliance. The BISC fosters a continuous government-to-government dialogue on information security essential to fully enabling the 2007 U.S.-Japan General Security of Military Information Agreement (GSOMIA), which governs the reciprocal protection of classified information.

"Our BISC efforts focus on protecting the partnership of the U.S. government and Japanese government by sharing our security practices," said Jenny Wells, executive program manager for DCSA Background Investigation Field Operations. Bilaterally, the BISC ensures that Japan's access to sensitive U.S. government information meets U.S. information security and personnel security standards. The same is true of U.S. access to Japan's sensitive government information. Substantial equivalency is crucial to ensuring that information shared between the U.S. and Japan remains secure. DCSA leaders – Marianna Martineau, Adjudications; Heather Green, Vetting Risk Operations (VRO); Ryan Dennis, VRO; Brian Sedor, Background Investigations; Charis Lyon, Adjudications; and Kim Knobel, Training – participated in detailed discussions with their Japanese counterparts to fulfill the requirements of the U.S.-Japan GSOMIA. Their advice and collaboration covered the treatment of information from operations to policies, technologies and technical data.

"The bilateral partnership with Japan is vital and a must win for both countries," said Richard Stahl, DCSA International and Special Programs chief responsible for bilateral agreements supported by the agency. "Success with BISC is essential not only to the GSOMIA but to our national security partnership as a whole."

DCSA's efforts with Japan began with a bit of shock in September 2019 when team members encountered

a typhoon that struck just before landing in Tokyo. "There was no way to leave the airport," Nelson recalled. "No buses, trains or cabs. It was an airport full of people panicking and looking for ways to leave."

In addition to DCSA and DTSA, the U.S. team included representatives from the Undersecretary of Defense for Policy; U.S. Forces Japan; the Department of State; the Department of Justice; the U.S. Embassy Tokyo interagency; and U.S. Indo-Pacific Command.

Fortunately, the team located tickets on the only bus to leave the airport for hours and met with their Japanese counterparts for the first time. The U.S. and Japanese teams would continue to work together to overcome challenges from language barriers to pandemic related restrictions and limitations.

"In our first trip, we provided the government of Japan with a high level overview of how the U.S. does federal personnel vetting and outlined the specific elements required under a U.S. background investigation," said Wells.

Overall, the U.S. team highlighted the fact that the U.S. government follows stringent policies and procedures out of a long history of conducting vetting for the federal government. The relevant subject matter experts briefed Japanese government officials and experts on the U.S. personnel security, vetting and adjudications system. In return, the Japanese leaders explained their information security system to the U.S. team.

"In December 2019, we came to Japan with a smaller contingent and conducted a formal assessment of Japan's information security practices," said Martineau, assistant director for DCSA Adjudications. "We followed the director of National Intelligence security protocol to assess the U.S. government's adequacy and applied that same methodology to our engagement with Japan."

Consequently, the Japanese and the U.S. teams were able to identify common expectations for key areas of information security.

"We constructed a framework to continue our engagement moving forward and stayed true to that framework," said Martineau.

The majority of work halted, however, at the beginning stages of the pandemic despite virtual meetings held by the U.S. and Japanese teams in their respective Washington and Tokyo locations.

> **"**Our BISC efforts focus on protecting the partnership of the U.S. government and Japanese government by sharing our security practices**"**
>
> ***~ Jenny Wells***

"It was a tremendous challenge to engage our counterparts through interpreters while attempting to keep the ball rolling via virtual engagements," she said. "It was really difficult."

In due course – specifically in October 2021 – the BISC teams reengaged to work together face to face in Tokyo.

"Great strides were made in terms of understanding each other's systems," said Charis Lyon, DCSA Adjudications Division 2 chief regarding the team's third BISC trip. Three months after DCSA enrolled DOD and some federal agencies into an initial version of the agency's Continuous Vetting Program, the third round of BISC meetings in Tokyo included DCSA briefings on continuous evaluation.

"Our counterparts in Japan have been really good partners in understanding our program and why the system of checks that we use are important," said Lyon. "They are active partners in that process and moving forward, we will continue advising each other."

In future BISC collaborations, the DTSA and DCSA team are planning to share with Japan the U.S. requirements outlined in the National Industrial Security Program Operating Manual (NISPOM).

"It was inspiring to see how the work we do every day impacts our partnerships and alliances around the world," said Brian Sedor, program manager for DCSA Background Investigations Quality Support. "Even though our security program continues to evolve to meet emerging threats, involvement in the BISC initiative makes me appreciate the current advanced state of our comprehensive security program."

Once the BISC engagements are complete, Nelson anticipates that DCSA Center for Development of Security Excellence representatives will exchange information with Japan's training professionals related to the agency's experience and capabilities in providing security education, training and professionalization for DOD and industry under the National Industrial Security Program.

ASK THE LEADERSHIP

A Question and Answer with the new DCSA Deputy Director

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

Daniel Lecce, Deputy Director

Daniel Lecce joined DCSA in January of 2022 as the Deputy Director. In this capacity, Mr. Lecce will be the principal advisor to the DCSA Director and will assist in shaping necessary policy, managing DCSA's resources, and leading operational activities to accomplish the agency's mission.

Mr. Lecce served 35 years in the United States Marine Corps retiring as a Major General. During his Marine Corps career, Mr. Lecce served in numerous high-level leadership positions both as a commander and advisor to high level Department of Defense leaders. In his last assignment, Mr. Lecce was responsible for the oversight, strategic direction, and resourcing of the Marine Corps' uniformed legal enterprise, leading a cadre of 1,500 military and civilian professionals located around the globe. During his tenure he led transformational change within the Marine Judge Advocate community driven by his strategy to optimize resources, establish training and fellowship programs, streamline processes and procedures, and introduce modern and fully secure information systems. As the senior-most uniformed legal advisor to the Commandant of the Marine Corps, Mr. Lecce provided strategic and service-related advice on issues including cyber law, intelligence-operations law, intelligence oversight, and military justice issues. He provided testimony to Congress on multiple occasions regarding high visibility issues facing the Marine Corps.

Mr. Lecce's prior experience also includes serving as the Commanding Officer of Marine Corps Base, Camp Lejeune, North Carolina. There, Mr. Lecce managed an operating budget of over $25 million, a military construction program valued at $3.5 billion and oversaw the largest facility and infrastructure expansion of the base since the 1940s.

Mr. Lecce also served as the Commander of Marine Security Guard units protecting 21 embassies and consulates across the Middle East and Asia. In that position, Mr. Lecce was responsible for Marines

overseeing the physical security of United States embassies and their personnel; safeguarding classified information; and responding to terrorist threats.

Mr. Lecce is a graduate of the University of Pittsburgh; the University of Pittsburgh School of Law; the U.S. Army Judge Advocate General's School; and the Johns Hopkins Nitze School of Advanced International Studies.

QUESTIONS AND ANSWERS

We have your biography, but is there anything in your background you would like to highlight for our readers?

I have experience leading a number of large enterprises during my career. In my last assignment, I led the transformation of the Marine Corps legal community comprised of 1,500 military and civilian professionals posturing the community to operate in a 21st century environment. DCSA is going through similar transformation so I am very eager to do my part to help our Agency through the challenges we are facing.

What brought you to this job?

Serving our country is very important to me. I strongly believe all owe a duty to serve our nation, an obligation I take very seriously. DCSA's mission is at the forefront of our national defense strategy. For example, protecting critical industrial technology is vital to the warfighter on the front lines. I have served with Marines in some very difficult situations and have seen firsthand how maintaining a technological advantage on the battlefield can be the difference between success and failure, life and death. What DCSA does in its various mission areas ties directly to the warfighter. Access to secure, uncompromised weapon systems are essential to the success of the Soldier, Sailor, Airman or Marine on the forward edge of defending our nation. Further, ensuring individuals in positions of trust are worthy of that trust is also key to our nation's success and security. DCSA's mission truly resonates with me and I feel very fortunate and privileged to have this opportunity to continue to serve and do our nation's work.

You have only been onboard a short amount of time, but what are your initial impressions of the agency?

My first impression has been that DCSA has a very strong, professional workforce from the senior leadership to the admin staff. I haven't been able to meet many people in person due to COVID restrictions, but I have been able to walk around the headquarters and introduce myself to those who are in the headquarters building. Everyone I have met has been extremely professional and hard working. I am very proud to be part of the DCSA team.

The position of Deputy Director has been vacant for some time. What will your duties/priorities be as Deputy Director?

One of my major areas of focus will be to help implement the five-year strategic plan for the Agency. We need to provide clear direction for our senior leaders, our customers, to include industry, and the DCSA workforce; everyone needs to understand where we're going. Concomitant with clear strategic direction, our communication must also be clear to ensure all are moving in the same direction and any concerns are addressed in a timely manner. Additionally, I want to focus on the DCSA culture. DCSA was established by bringing a number of different agencies together in order to execute a single mission. Establishing an agency culture is important to reinforce ownership, pride, and common purpose in our organization.

How do you see your role supporting/complementing that of the Director?

I add value by providing the Director the time to operate effectively at the strategic level within DOD, with our external partners, and with Congress. I expect to focus more on the day-to day-tasks of the Agency. DCSA can make great strides, especially in resourcing, with an enhanced focus on strategic engagements. My role will be to give the Director the time and room to do that.

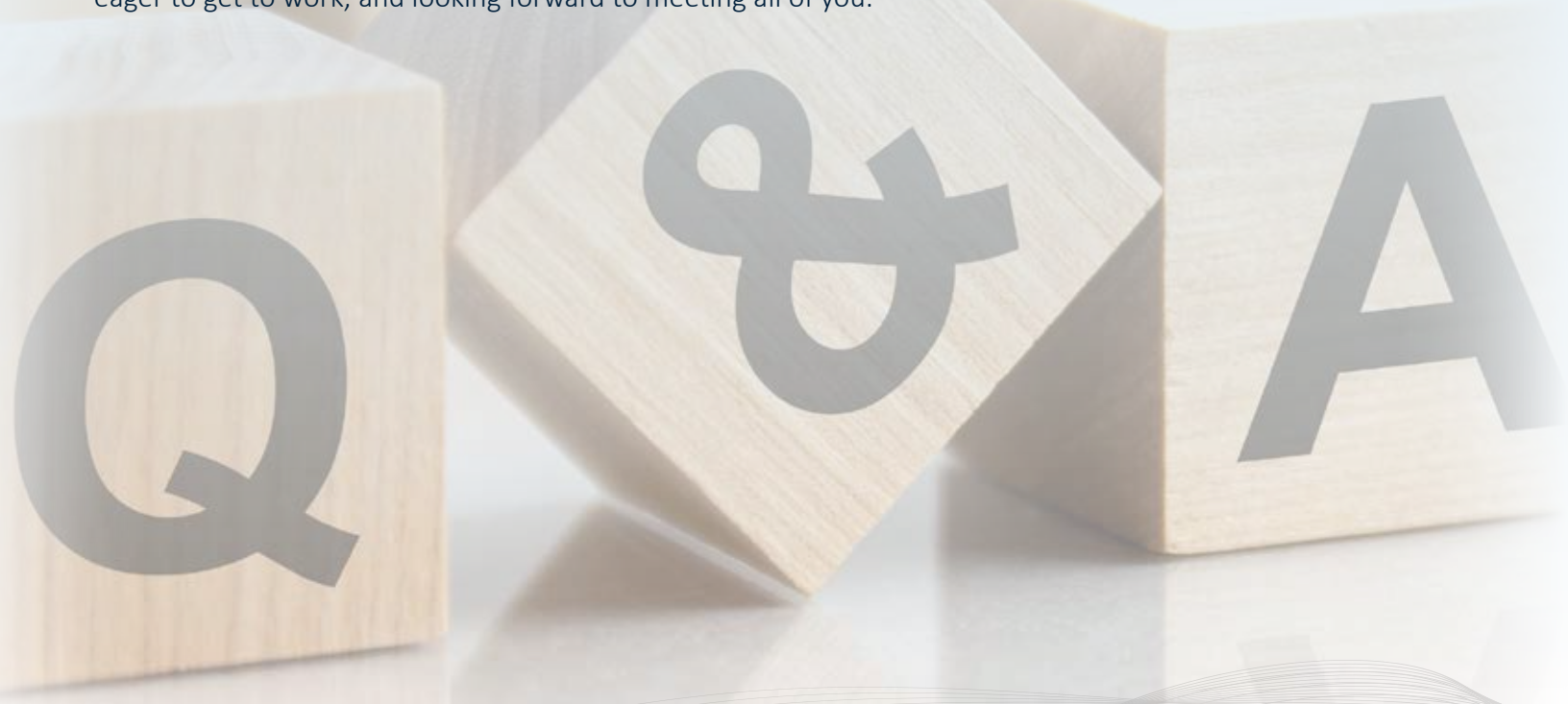
You've held various leadership roles during your military career. What are some of your "best practices" that you'll bring to this job?

First, take care of your people. You have to care for your people or you won't get very far. That is job number one; to ensure this group of dedicated and hard-working people are being heard, recognized, and taken care of. It's difficult with such a dispersed workforce. In my experience, a headquarters can become inwardly focused and you lose sight of those doing the hard work in the field. We must recognize our people for the good work they do; that's a key component. In the coming months, as COVID restrictions lessen, the Director and I look forward to traveling more to visit our team in the field.

Second, you must have a plan, especially during times of change and transformation as we are experiencing at DCSA. The plan must be deliberate, clearly communicated, executable, and achievable to ensure efficiency and unity of action. You can't over communicate. The team must understand where we're going. At the same time, we must maintain a strong feedback mechanism at all levels to ensure all concerns are addressed and best practices are implemented. We have a wealth of experience and knowledge in DCSA that must be leveraged to our advantage. We also must be open to new ideas and be agile enough to adjust when necessary.

Are there any final thoughts you would like to share with our readers?

I consider it a great privilege and honor to continue to serve our nation. I have met some true professionals in my short time at DCSA and I know they share my commitment to our nation and our mission. I'm looking forward to getting out to the field and meeting the team and receiving their input. I am very excited to be here, eager to get to work, and looking forward to meeting all of you.



DCSA STRATEGIC PLAN 2022-2027
OUTLINES NINE GOALS TO COLLECTIVELY ACHIEVE AGENCY MISSION VISION

By Wally Coggins
Chief Strategy Office

Since its stand up in October of 2019, DCSA has been on a multi-year transformation journey, with the merging of eight distinct organizations or parts of organizations into the agency. Today, DCSA boasts a workforce of about 10,000 government employees and contractors, and works out of over 160 regional and field offices throughout the United States. This physical presence embeds the DCSA workforce on the front lines of the effort to protect the Defense Industrial Base (DIB) and the trusted workforce for the Federal government.

DCSA's missions are expanding and evolving to meet customer expectations, with new policies such as the Government-wide transition to Trusted Workforce 2.0, the implementation of National Defense Authorization Act Section 847 beneficial ownership provisions, and increased demand for security training and threat assessments for cleared industry partners. The rapidly changing threat environment characterized by great power competition, increasingly sophisticated information technology and cyber activity, and emerging domestic extremism and insider threats require that DCSA optimize its performance. While agency leaders have been focused on delivering their respective missions, they have also been collaborating with internal and external stakeholders to build a Strategic Plan that will set the agency's direction for the next five years. The 2022-2027 Strategic Plan aligns with broader intelligence and defense strategies and lays the foundation to accommodate DCSA's expanding missions. It will guide and align DCSA's efforts to transform in order to deliver its Gatekeeper mission.

SHIFTING FROM A TRANSFORMATION-FOCUSED STRATEGIC FRAMEWORK TO A FIVE-YEAR STRATEGIC PLAN

The strategic plan was not built from scratch. After DCSA's inception in 2019, the agency built a DCSA future state Operating Model (OpModel), and the Strategic Framework to provide the interim guidance needed to align and prioritize transformation initiatives while merging organizations.

The Strategic Framework drove a range of transformation activities that laid the foundation needed to align as an agency to execute a five-year strategic plan with direction and purpose. Under the strategic framework, DCSA had several accomplishments that supported both mission and enterprise delivery:

- Implemented the Trusted Workforce (TW) service (TW 1.25), enrolling DOD and non-DOD agencies into this first TW continuous vetting service

- Developed a Security Risk Management Capability Concept of Operations to support information sharing and inform a common understanding of the risks across missions.

- Drove field transformation, which included the establishment of new regional boundaries, a decision regarding new headquarter locations, and a new regional organizational structure.

- Developed a Customer Experience Strategy that will guide the development of customer-centric capabilities

- Released a new Data Strategy, and established the Enterprise Performance Management program to support effective definition, monitoring, and measurement of progress against its mission execution goals.

These projects are a snapshot of many transformation activities that position DCSA to effectively carry out its new strategic plan.

THE FOUNDATION OF THE STRATEGIC PLAN

The 2022-2027 Strategic Plan identifies nine goals that will collectively help the agency achieve its mission and vision. These nine goals are divided into two categories: mission goals and enterprise goals. Mission goals will advance mission performance through unity of effort, partnership, and customer experience, and directly align to the four mission areas of the Agency OpModel: Industrial Security, Personnel Security, Threat, and Training. Enterprise goals cut across the entire agency to empower the workforce and deliver capabilities that support more effective business operations and improve overall mission performance.

DCSA MISSION

Through vetting, industry engagement, education, and counterintelligence and insider threat support, secure the trustworthiness of the United States government's workforce, the integrity of its cleared contractor support, and the uncompromised nature of its technologies, services, and supply chains.

VISION

Optimize our performance as the preeminent security organization to protect our Nation's critical assets through enterprise risk management, continuous innovation, and excellence in mission performance and customer service.

MISSION GOALS

INDUSTRIAL SECURITY: ENABLE THREAT REDUCTION AND MITIGATE VULNERABILITIES TO CLASSIFIED AND SENSITIVE INFORMATION AND TECHNOLOGY IN THE U.S. INDUSTRIAL BASE

DCSA will develop and validate new Industrial Security capabilities and requirements, invest in technology, and share information with appropriate stakeholders. Actions to achieve this goal will enable DCSA to mitigate risks in the cleared contractor base and introduce new procedures and mature its risk-based approaches. It will also position DCSA to become a pivotal partner in securing the Defense Industrial Base, beyond the cleared contractor base.

PERSONNEL SECURITY: IDENTIFY AND MITIGATE PERSONNEL-BASED THREATS WHILE ENABLING CUSTOMERS TO ONBOARD TALENT QUICKLY

DCSA will implement the Trusted Workforce policy framework and continue to be the premiere provider of personnel vetting services for the Federal Government. DCSA will meet established investigation timelines while maintaining high-quality investigative services the agency has always delivered.

COUNTERINTELLIGENCE AND INSIDER THREAT: IDENTIFY, INTEGRATE AND SHARE THREAT INFORMATION ACROSS THE ENTERPRISE TO HELP DRIVE RISK-BASED, DATA-DRIVEN DECISIONS AND ACTIONS

DCSA will deny and disrupt strategic competitors and trusted insiders' malicious intent through analysis of information and intelligence, the execution of counterintelligence functional services, and the management and oversight of the insider threat enterprise. DCSA will collaborate with mission partners, cleared industry, and other government agencies to detect, deter, assess, disrupt, and mitigate counterintelligence, cyber and insider threats.

SECURITY TRAINING: TRAIN US GOVERNMENT, INDUSTRY, AND AGENCY PERSONNEL TO MITIGATE RISK IN SUPPORT OF NATIONAL SECURITY

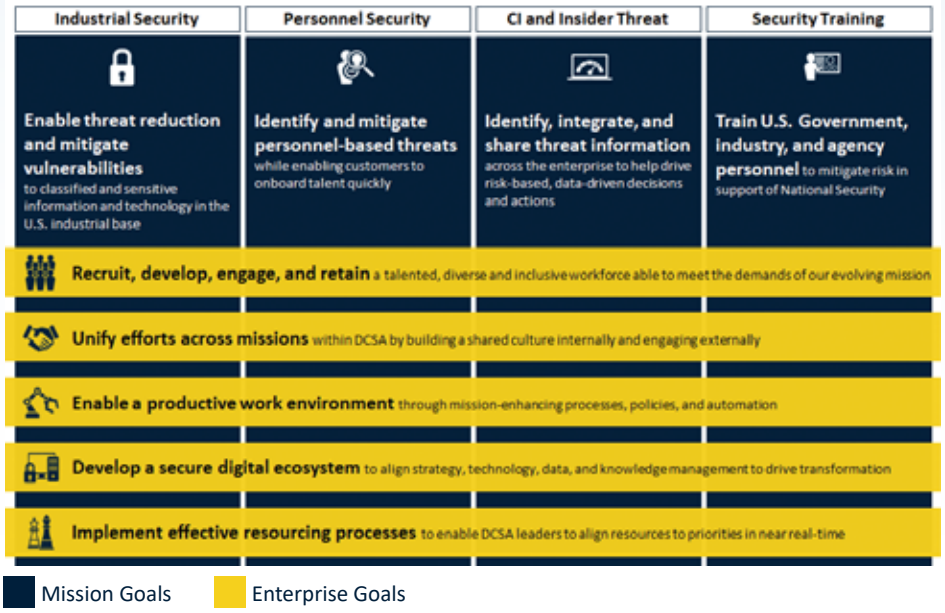
The agency will leverage technology to improve the content and accessibility of our training material and ensure the customer experience is characterized by rapid and timely delivery of critical information precisely where and when it is needed. Additionally, DCSA will focus on expanding its customer base for training products and services and leveraging them for the purpose of mitigating security risks wherever they might be found.

ENTERPRISE GOALS

TALENT: RECRUIT, DEVELOP, ENGAGE, AND RETAIN A TALENTED, DIVERSE, AND INCLUSIVE WORKFORCE ABLE TO MEET THE DEMANDS OF OUR EVOLVING MISSION

DCSA will build its workforce through recruiting diverse, qualified talent and through workforce development. DCSA will incorporate new technologies and methodologies to support data-driven strategic workforce planning and decision-making processes across the agency. DCSA will focus on cultivating collaborative leaders who can help their teams contribute towards the goal of a unified organization and mission success.

Five Year Strategic Goals (2022–2027)



UNITY OF EFFORT: UNIFY EFFORTS ACROSS MISSIONS WITHIN DCSA THROUGH BUILDING A SHARED CULTURE INTERNALLY AND ENGAGING EXTERNALLY

DCSA must move from a collection of missions that operate in siloes to security missions working collectively as a single agency. DCSA will build strong partnerships and a commitment to consistent communications about the agency's priorities and activities and clear guidance on cross-mission information sharing parameters, and will raise awareness of its mission impact across customer, industry partners, and stakeholders.

OPERATIONAL EFFECTIVENESS: ENABLE A PRODUCTIVE WORK ENVIRONMENT THROUGH MISSION-ENHANCING PROCESSES, POLICIES, AND AUTOMATION

This strategy focuses efforts to work more productively on behalf of the nation. It will reduce administrative burdens on the agency's workforce through investments in technology that reduce manual processes.

DIGITAL ECOSYSTEM: DEVELOP A SECURE DIGITAL ECOSYSTEM TO ALIGN STRATEGY, TECHNOLOGY, DATA, AND KNOWLEDGE MANAGEMENT TO DRIVE TRANSFORMATION

DCSA will create networks that are more secure and resilient by developing dynamic digital protection capabilities and a cybersecurity framework to prevent data breach of applications and systems. This will ensure that data is available to those who need it, when they need it.

RESOURCING PROCESSES: IMPLEMENT EFFECTIVE RESOURCING PROCESSES TO ENABLE DCSA LEADERS TO ALIGN RESOURCES TO PRIORITIES IN NEAR REAL-TIME

DCSA will mature its decision management processes for requirements, resourcing, and acquisitions. This will result in financial resources being allocated in support of validated requirements to drive strategy execution.

INFORMED DECISIONS AND PERFORMANCE REPORTING

The DCSA Strategic Plan will be the "center of gravity" as the agency monitors Key Performance Indicators, resource requirements, transformation initiatives, and other key components of its operations. Each goal will have a champion who will be responsible for building and executing a plan to deliver specific milestones each fiscal year. Every year, the agency will conduct an annual strategic planning process to revisit initiatives and determine how it will continue to meet its strategic goals and objectives, informing the Program Objective Memorandum (POM) process. Additionally, the agency will align its current transformation projects to newly identified strategic goals and objectives, and determine strategy integration with the new governance structure. The agency's five-year strategy brings together diverse mission areas and focuses their efforts into synchronized action. This unified effort allows the agency to successfully protect the nation's most important information and its trusted workforce.

AGENCY OFFICIALLY CHARTERS PROGRAM EXECUTIVE OFFICE, NINE PROGRAM MANAGERS IN CEREMONY

By Sean Kunzler
Chief of Plans and Operations, Program Executive Office

On November 30, 2021, DCSA made history when it conducted an inaugural Program Executive Office (PEO) Charter Ceremony. DCSA Director William K. Lietzau, in his capacity as DCSA's Component Acquisition Executive (CAE), officially chartered the Program Executive Officer, the Executive Program Manager (EPM) of the National Background Investigation Services (NBIS), and eight other program managers, observing a symbolic tradition of transition and transformation.

In 2019, the Deputy Secretary of Defense directed the transfer of several personnel and industry security systems and services into the new agency-- DCSA. The new mission required an acquisition capability to unify a myriad of diverse information technology development programs transitioning from across the Federal government. As a DOD component with acquisition authority, DCSA looks to the PEO to manage these capabilities.

The DCSA PEO was formally established on Oct. 1, 2020. On that same date, the NBIS program transitioned from the Defense Information Systems Agency (DISA), as did eight other programs that would constitute the PEO.

During the ceremony, Lietzau presented Terry L. Carpenter Jr. with the PEO charter, recognizing and authorizing him as the first Program Executive Officer for the agency. As the Program Executive Officer, Carpenter "balances the risk, cost, schedule, performance, interoperability, sustainability, and affordability of a portfolio of acquisition programs and delivers an integrated suite of mission effective capabilities…"

"I'm honored to be a part of this team of fantastic acquisition professionals who came from many different places bringing a variety of experience," said Carpenter. "They all understand the responsibility they are taking on."

DCSA Director William K. Lietzau (left) presents Terry L. Carpenter, Program Executive Officer, with the PEO charter.
(Photo by Christopher P. Gillis, OCCA)

Lietzau also officially chartered Jeffery S. Smith as the EPM NBIS, currently the flagship acquisition program in the agency. As the EPM, Smith manages the federal government's integrated information technology system for comprehensive personnel vetting — from initiation and application to background investigation, adjudication, and continuous vetting.

"I couldn't do it without the support of my team," said Smith who encouraged them to "stay the course and keep reaching for the stars" regarding the ongoing design and development of NBIS in spite of challenges such as working virtually during the pandemic.

Carpenter then chartered the eight PEO PMs. The PMs plan acquisition programs, prepare programs for key decisions, and execute approved acquisition and product support strategies, and ensure cost, schedule, and performance objectives are accomplished. PMs are charged with tremendous responsibility to manage and oversee major defense acquisition programs in accordance with acquisition policy, regulations, and statutory law.

> I'm honored to be a part of this team of fantastic acquisition professionals who came from many different places bringing a variety of experience.
>
> They all understand the responsibility they are taking on.
>
> ***~ Mr. Terry Carpenter***

DCSA Director William K. Lietzau (left) presents Jeffery S. Smith, Executive Program Manager, National Background Investigation Services, with the NBIS charter.
(Photo by Christopher P. Gillis, OCCA)

"The program reflects your personality and your ability as a leader," he told the eight PMs. "The program team looks to you in a time of crisis and stress and your obligations are huge. It's a duty that richly deserves the honor and title program manager. It is your turn to lead. Today you assume your command."

The eight PMs are:

Leonard Mierzwa, as PM Biometrics, develops and maintains underpinning identity services required by the DCSA mission systems. This program is evolving services in alignment with DoD and industry innovations in biometrics and identity management.

Christopher Carrigan, as PM Cloud Services and Data Management, provides a common platform for all DCSA IT systems to develop, operate and secure data in support of DCSA missions.

Charles Washington, as PM DOD Insider Threat Management and Analysis Center System of Systems, provides program management for the development and sustainment of the IT system for the DITMAC.

Diane Brooks-Woodruff, as Enterprise Services Delivery, provides program management for the development and delivery of cloud-based back-office services that reduce administrative burdens for internal and external DCSA stakeholders to perform day-to-day business operational functions.

Bruce Hunt, as PM Robotics Process Automation, provides short and long term agile custom business solutions and robotic process automations capability to support efficiencies for DCSA.

Geoffrey Hart, as PM Security Education and Training System, provides program management for the development and sustainment of the portfolio of seven systems that enable the security education and training of DOD and other Mission Partner Workforce.

Renee Esposito (former) and subsequently Ron Blanch, as PM Background Investigation Enterprise Systems (BIES), manages the operations, security and maintenance of the legacy OPM IT system providing security clearance background investigations. PM BIES will implement sunset of the systems in preparation for full NBIS deployment.

"I'm very comfortable and confident in our program manager team. This is a huge success for DCSA – building this team and giving a mantle of responsibility and authority to the people you see here," said Lietzau. "I want to thank them for the responsibilities that they are taking on and have already taken on."

Chartering of the PEO and PMs solidifies their autonomy to make decisions to respond to requirements and deploy systems that bring value and enable the agency mission. This officially establishes the undertaking at hand and grants those bestowed, the authority to command the responsibilities as they see fit.

DNI CLARIFIES GUIDANCE ON MARIJUANA POLICY IMPACTING SECURITY CLEARANCE ELIGIBILITY, ADJUDICATION

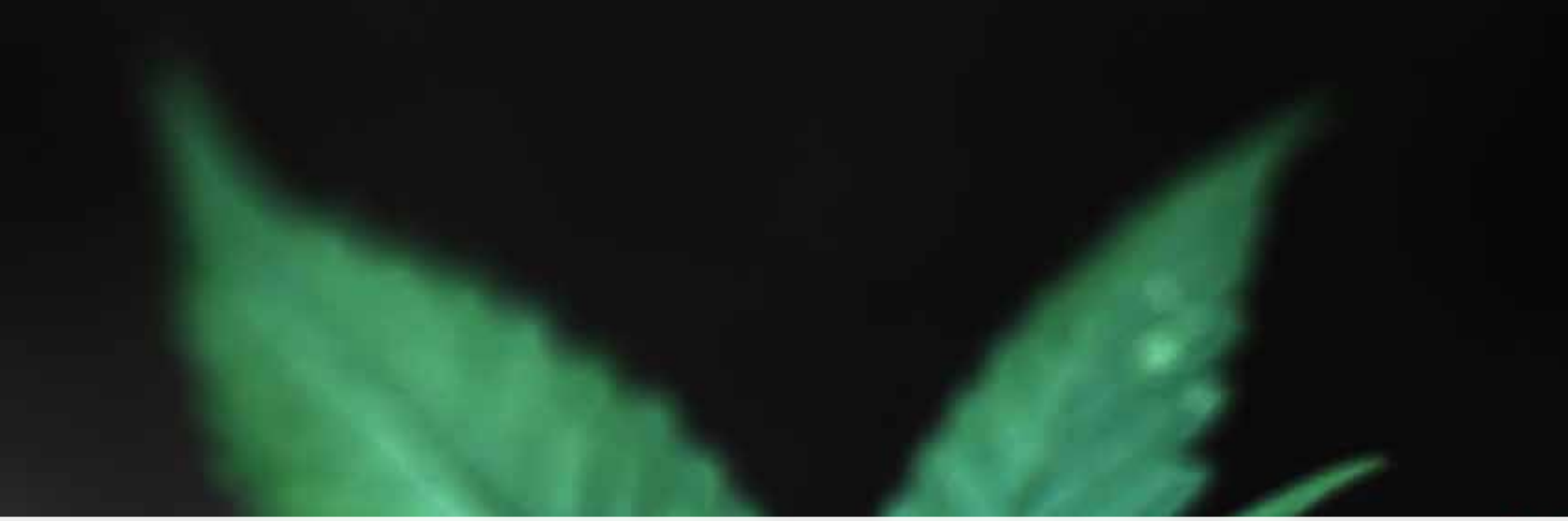
Director of National Intelligence Avril Haines released a memorandum throughout the federal government on Dec. 21, 2021, clarifying DNI's guidance on how marijuana use and investment impacts security clearance eligibility and adjudicative determinations.

The memorandum – "Security Executive Agent Clarifying Guidance Concerning Marijuana for Agencies Conducting Adjudications of Persons Proposed for Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position" – signed by Haines as security executive agent, is a reminder and clarification of longstanding DNI guidance regarding security clearance eligibility and adjudicative determination amid the growing number of state and local governments that are decriminalizing recreational marijuana.

"I encourage agencies to remind civilian, military, and contractor personnel, who are eligible for access to classified information or eligible to hold a sensitive position as well as authorized investigative and adjudicative personnel, of the importance of continued adherence to federal laws and policies, to include adhering to applicable reporting requirements," said Haines in the memorandum. "The illegal use or misuse of controlled substances can raise security concerns about an individual's reliability and trustworthiness to access classified information or to hold a sensitive position, as well as their ability or willingness to comply with laws, rules, and regulations. Drug involvement may raise similar concerns about personal and criminal conduct."

Although recreational marijuana use remains illegal at the federal level and continues to be prohibited while a person occupies a sensitive position or holds a security clearance, the guidance emphasizes that it should not be determinative in making adjudicative decisions.

Moreover, the DNI clarification encourages agencies "to advise prospective national security workforce employees that they should refrain from any future marijuana use upon initiation of the national security vetting process, which commences once



the individual signs the certification contained in the Standard Form 86 (SF-86), Questionnaire for National Security Positions."

In addition to the potential consequences of recreational drug use in security clearance determinations, the guidance addresses the use of cannabidiol (CBD) products and investments in marijuana-related businesses by clearance holders.

The guidance states that CBD oils with greater than .3% of tetrahydrocannabinol (THC) continue to meet the legal definition of marijuana. It reminds clearance holders and adjudicators that security clearance eligibility for persons who intentionally invest in marijuana businesses may be impacted negatively. However, it emphasizes that indirect investment through a diversified mutual fund should not be considered relevant for adjudications.

"The DNI clarification is in concert with and meaningfully underscores existing DCSA Adjudications operational adjudicative policy and practice," said Richard Weyrauch, DCSA Adjudications Division 7 chief. "Marijuana use and the presence of THC in drug testing, possession, production and distribution continue to be potentially disqualifying. SEAD 3 (Reporting) and SEAD 4 (Adjudication) remain unchanged."

Weyrauch added that the clarification about an adjudicative determination potentially being negatively impacted if an individual knowingly and directly invests in stocks or business ventures pertaining to marijuana growers and retailers has not changed and is consistent with existing policy and practice.

"The DNI memo clarifying guidance concerning marijuana use helps security managers reemphasize federal policy to their national security workforce," said Amanda Collado-Milligan, DCSA Personnel Security senior program coordinator. "Although the social taboos surrounding marijuana have relaxed, the use or presence of marijuana, including THC, continue to be potentially disqualifying and require reporting."

PROGRAM EXECUTIVE OFFICE LAUNCHES NEW ACQUISITION AND BUDGET MANAGEMENT TOOL

By Joseph Wagner
Program Executive Office

In support of the agency's transformation efforts, the Acquisition and Budget Management (ABM) application is a user-friendly, centralized application that is modernizing how DCSA manages spend plans by transitioning manual processes into automated workflows. Through ABM, DCSA is on the path to realizing standardized agency-wide budgets, full financial transparency and auditability, and more efficient lifecycle tracking and reporting across mission areas.

WHAT DROVE THE NEED FOR STANDARDIZATION?

In 2019, when multiple organizations combined to form DCSA, it opened both a need and opportunity to modernize and standardize financial and acquisition processes.

This need was acutely felt by the Program Executive Officer (PEO), Terry Carpenter, who sought to keep his finger on the pulse of the PEO's spend while interweaving industry best practices to help him make more informed decisions. With this challenge in mind, Dan Davis, PEO Acquisitions & Resources (A&R) Strategic Management & Analytics Division chief, began exploring an opportunity to leverage technology for the agency.

"My initial goal was to improve the ability to collect spend plan data and analyze it," said Davis. "I wanted to be able to tell leadership exactly how their money was being spent so they could make the right business decisions going forward."

During the incubation period within the PEO, the application was demonstrated to DCSA's new Chief Financial Officer (CFO) Zack Gaddy. He recognized that the modernization and standardization occurring in the PEO aligned with his goals for the financial maturity of DCSA. By taking on the role of Executive Sponsor for ABM, Gaddy enabled the OCFO to utilize technology to continue its path to financial transparency, standardize additional processes, and align the agency to industry best practices for financial management. As a result, ABM was rolled out agency-wide in fiscal year 2022 (FY22).

WHAT IS THE ACQUISITION AND BUDGET MANAGEMENT (ABM) APPLICATION?

ABM, built in the ServiceNow Platform, uses modernized, automated workflows to streamline the budget and contract approval process. The streamlined process reduces the number of hours of manual data entry, prevents packages from being lost in email communications, and allows all stakeholders to see exactly where requests are in the approval process.

In addition, ABM promotes full lifecycle tracking and easy reporting across mission areas through a central data repository and a user-friendly interface. ABM allows for the development of performance metrics for directorates to assist with investment decisions and benchmarking. With the power of a central data repository, users can access the data to forecast upcoming funding actions or future budget shifts, enabling the agency to become more proactive rather than reactive.

WHERE ARE WE NOW?

The agency-wide ABM application successfully launched in October 2021, providing an automated tool that streamlines DCSA budget and acquisition workflows and empowers users to execute their funding needs and track spending in real time. Since inception, the ABM team sought to support the user adoption and user experience through the creation of standard operating procedures, training guides,

> I wanted to be able to tell leadership exactly how their money was being spent so they could make the right business decisions going forward
>
> ~ *Mr. Dan Davis*

one-pagers, recorded video demonstrations, and the ABM Tool Digest newsletter to communicate the application's capabilities and answer frequently asked questions. Additionally, ABM has continued to evolve with key stakeholder support from Acquisition and Contracting (AQ), CFO, and Chief Strategy Office (CSO) mission areas to enhance functionality, scalability, and adoption across the agency.

This capability enables DCSA to track its nearly $2 billion budget by creating a centralized data repository of historical and future year data, which allows for greater precision in budget forecasting and robust reporting and data visualizations. Through the collaboration with CFO and AQ, ABM is integrating financial information at a more granular level – providing leaders with a new lens to support strategic decisions that impact the agency's financial future. Additionally, ABM data is facilitating the new timekeeping process realignment driven by CSO. This combined with the efficiencies gained through enhanced workflows is helping to streamline the financial process for budget users across DCSA.

Through the partnership with AQ, a Contract Request workflow allows program analysts to submit packages to be simultaneously reviewed by AQ (package requirements) and FM (funding availability) directly in the tool – establishing one connected, end-to-end process across stakeholder groups.

To date, ABM is actively used by 400+ program analysts, financial managers, and acquisition specialists performing modernized budget and acquisition processes, with an additional 1,700+ users submitting Miscellaneous Reimbursements through the tool.

Following ABM's successful FY22 launch, an ongoing evaluation is being conducted to determine future expansion opportunities through user feedback and process changes. For FY22, ABM will enhance existing capabilities and expand functionality to become a multi-dimensional platform that reports agency budget controls, tracks directorate spend plans and execution progress, and manages all current and future budget and acquisition workflows.

Looking ahead, this multi-dimensional single platform will be achieved through a series of future enhancements developed in partnership with mission areas across the agency. The ABM team is working with stakeholders to enhance several budget and contract related workflows in the tool (e.g., for Inter Agency Agreements and Government Purchase Cards). Legacy manual forms, such as the Standard Form 231, will be automated through the advent of digital authentication capabilities within the tool. A Spend Plan Formulation capability currently in development will enable directorates to view their budget controls, historical data, and latest spend plan execution data to create their next year spend plan. Further, additional DCSA AQ capabilities will be launched to expedite acquisitions operations and provide visibility into contracting resource management. As the financial data in the tool continues to be refined, automated dashboards and reporting capabilities will be further enhanced to provide DCSA decision makers with informative, real-time data, allowing them to make better informed decisions that will influence the future direction of the agency.

"In February, over 35 personnel from the CAF were onboarded into the NBIS Operational Test environment, also known as the "NBIS Playground."

DCSA ADJUDICATORS TRANSITIONING OPERATIONS TO NBIS PLATFORM

By Charis Lyon
DOD Consolidated Adjudications Facility

What is NBIS? The National Background Investigation Services (NBIS) is the federal government's end-to-end information technology system for personnel vetting. NBIS will be used for initiation, application submission, background investigation, adjudication, and continuous vetting; an all-in-one consolidated system. Smaller federal, non-Department of Defense agencies are currently onboarding into NBIS.

The DOD Consolidated Adjudications Facility (CAF) is working hand-in-hand with the NBIS team to plan for the phased transition of adjudications from the Defense Information System for Security (DISS) to NBIS. Several working groups are developing actionable items between CAS and the NBIS team: Training, Workflow Configuration, Due Process Procedures, Organizational Structure, Case Tagging, Metrics/Reporting and Suitability/Homeland Security Presidential Directive-12 Process. These items are discussed during bi-weekly NBIS-Adjudications planning sessions.

In February, over 35 personnel from the CAF were onboarded into the NBIS Operational Test environment, also known as the "NBIS Playground." In the NBIS Playground, CAF personnel will perform end-to-end testing of the adjudications workflows within the system. Results will inform any configuration adjustments or future requirements. The end-to-end testing will occur on a weekly basis and involve CAF, Security, and NBIS team personnel. The NBIS team will be available to the adjudicators for training, questions, and troubleshooting.

By April, approximately four to six adjudicators from the CAF will be on boarded into the NBIS Production environment. These adjudicators will use NBIS to adjudicate DCSA military, civilian, and contractor cases. In order to adjudicate within NBIS, these cases will need to be replicated from DISS to NBIS. The DCSA Security Office is already onboard in NBIS and as a result, DCSA adjudicators will be able to send subject-based communications to the DCSA Security Office via NBIS.

As more customer agency security offices onboard into NBIS for initiation and subject management, the CAF will increase its presence in the production environment to execute adjudications for those agencies. During this phased entry into NBIS, the CAF is excited to learn how NBIS works and translate that into expectations for the broader workforce as more personnel are brought into the system.

MODERNIZING PERSONNEL VETTING:
TRUSTED WORKFORCE 2.0 IMPLEMENTATION OFFICE COORDINATES EFFORTS

By Ashley Sarna, Adjudications, and Christie Larson, Chief Strategy Office

The personnel vetting program has evolved over the decades as new threats were identified, but the underlying framework remains the same. To address today's more expansive and complex threat, mission, workforce, and capability protection needs, personnel vetting requires transformational reform.

In March 2018, the Performance Accountability Council (PAC) convened Executive Branch, Congress, academia, and industry leaders for a two-day gathering. Participants expressed a commitment to reform and fundamentally overhaul Federal personnel vetting. Together, they chartered the boldest personnel vetting reform in decades – Trusted Workforce 2.0. The goal of TW 2.0 is to support agencies' missions by reducing the time required to bring new hires onboard, enable mobility of the Federal workforce, and improve insight into workforce behaviors, while ensuring the protection of people, property, information, and mission. An article in the January issue of the DCSA Gatekeeper magazine captured the details of TW 2.0, and serves as an excellent summary of the upcoming changes.

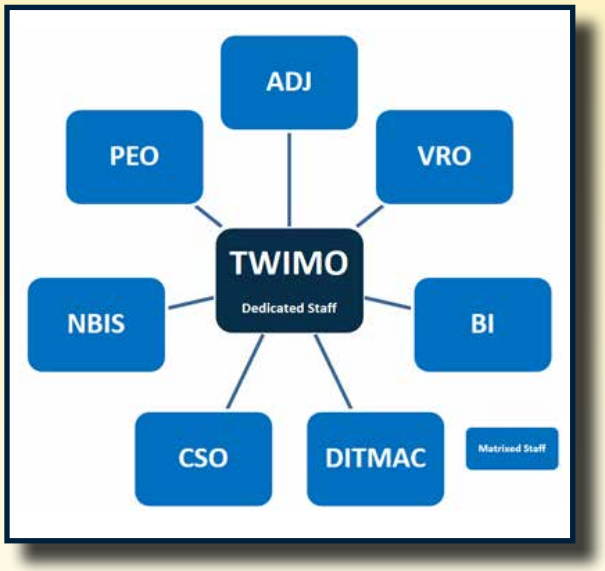
Through recent guidance, the Biden-Harris Administration continues to champion reform efforts with National Security Memorandum 3, which sets out assessing personnel vetting reform as an administration priority. This has elevated the effort throughout government and established the PAC as the National Security Council's Interagency Policy Committee, and means Defense Counterintelligence and Security Agency's (DCSA's) progress in this area will be reported to the President.

TW 2.0 will impact every individual within our agency and all of government, in support of DCSA's mission, to secure the trustworthiness of the United States Government's workforce, the integrity of its cleared contractor support, and the uncompromised nature of its technologies, services, and supply chains through vetting, industry engagement, counterintelligence support, and education. To meet this challenge, DCSA Director William K. Lietzau approved the plan coordinated across vetting seniors to stand up DCSA's Trusted Workforce Implementation Management Office (TWIMO).

In addition to a central office staff, full-time TWIMO representatives are matrixed from several DCSA mission areas, to include: Adjudications, Background Investigations, Vetting Risk Operations, Chief Strategy Office, Program Executive Office, DOD Insider Threat Management and Analysis Center, National Background Investigation Services, and others. Together this team is coordinating DCSA's TW 2.0 implementation efforts. The TWIMO is structured to leverage DCSA's greatest asset, the subject matter expertise of its mission specialists. As Trusted Workforce planning and implementation tasks are required, the representatives will reach back within their respective organizations to ensure all equities and mission impacts are accounted for. While the central TWIMO seeks to keep its efforts aligned and focused on the TW 2.0 finish line, the mission representatives are key to guaranteeing there will be no working level breakdowns when the policy begins to impact mission activities.

The TWIMO

The TWIMO maintains stakeholder engagement, focuses strategic planning efforts, assesses risks, analyzes potential pain points in implementing TW 2.0, monitors performance to better align with new policies, and streamlines coordination with PAC efforts to put DCSA in the best position to achieve results. They work closely with the Executive Agents (EAs) and PAC PMO to ensure alignment with the enterprise strategy. Since its inception in August 2021, the TWIMO's efforts have focused on initial high-level planning for the implementation of TW 2.0, identifying the steps and associated timelines that will be necessary for DCSA to be successful. In addition, the TWIMO has taken lead on the coordination of feedback from across DCSA in response to TW 2.0 related policy and strategic planning efforts from the EAs and the PAC PMO. From spring 2022 and forward, the TWIMO will shift from a planning focused group to a TW 2.0 implementation coordination and tracking entity.



The TWIMO will ensure that TW 2.0 planning and implementation efforts are successful and support DCSA's vision to optimize performance as the preeminent security organization, protecting the nation's critical assets through enterprise risk management, continuous innovation, and excellence in mission performance and customer service. The dedication of the TWIMO team will drive personnel vetting reform and contribute greatly DCSA's mission of protecting national security.

U.S. Air Force photo by Airman 1st Class Jose Miguel T. Tamondong

PARTNERSHIP BETWEEN F-35 JOINT PROGRAM OFFICE, DCSA TAKES FLIGHT

By Darren Denard, Industrial Security Directorate, and John Rhodes, F-35 Industrial Security Manager

In August 2021, a meeting was held between DCSA, the F-35 Joint Program Office (JPO), and the Air Force Office of Special Investigations (AFOSI), at the DCSA Irving Field Office in Irving, Texas, to discuss common security interests related to the F-35 Lightning II program. The August meeting was part of an initiative between the Irving Field Office and the F-35 JPO to take a more holistic and collaborative security oversight approach to resolve the program's complex security challenges and confront the current threat environment.

All three government entities have security cognizance roles at Lockheed Martin Aeronautics Company (LMAC), the primary manufacturing site of the F-35 in Fort Worth, Texas. LMAC is the prime contractor, with principal partners Northrop Grumman and BAE Systems. The F-35 JPO has been delegated with security oversight for the F-35 Program from the Defense Technology Security Administration (DTSA) for foreign industry partners. Over the years, DCSA Irving and the JPO have cooperated on common interests to provide government oversight for LMAC through teleconferences, but the August 2021 meeting was the first time these representatives from DCSA Irving and the JPO met in person. The Irving Field Office attendees included Jennifer Norden, Field Office Chief; Tyrone Baker, Information Systems Security Professional Team Lead; and Darren Dennard, Senior Industrial Security Representative (SISR). The Central Region leadership also supported this meeting via teleconference: Regina Johnson, Regional Director; William Vaughan, Authorizing Official; Matt Blakley, Assistant Regional Director; and Jessica Quigley, Senior Regional Action Officer. Representing the JPO were Robert Proud, JPO Deputy Security Director; John Rhodes, JPO Industrial Security Manager; and Aaron Garcia, AFOSI Program Security Officer – Counterintelligence.

The meeting at the field office was productive in identifying potential ways to strengthen oversight and support of the program throughout the program's acquisition life cycle. The visit to the field office was followed by two more days of discussions at the LMAC facility in Fort Worth.

During the visit, Rhodes recognized DCSA would greatly benefit from experiencing the larger international footprint of the F-35 manufacturing environment. In September 2021, Dennard, the DCSA SISR assigned to LMAC, accompanied Rhodes and his team on a visit to the F-35 Final Assembly and Checkout Facility (FACO) in Cameri, Italy. Dennard spent a week observing as Rhodes, his team, and DTSA representatives worked with the Italian Ministry of Defense and the Italian National Security Authority to get this facility in compliance with security requirements as a certified FACO for the F-35 Program. The trip provided Dennard with a greater understanding of the F-35 Program and the role of LMAC in the program.

Since returning from Italy, Rhodes has accepted an invitation to participate as an observer during the next DCSA security review scheduled at the LMAC Fort Worth site this year. Further, with the assistance of the Irving Field Office, the JPO Security Team is actively pursuing similar collaborative relationships with other DCSA Field Offices with F-35 cognizance.

U.S. Air Force photo by Tech. Sgt. Nicolas Myers

ACQUISITION AND CONTRACTING: CHANGING TO MEET NEEDS OF DCSA

The Defense Counterintelligence and Security Agency (DCSA) Acquisitions and Contracting Office continues to expand and transform by leaps and bounds since contracting offices from two major federal agencies – Defense Security Service and the National Background Investigations Bureau – consolidated as one team within a new agency in October 2019.

The state of growth and transformation at DCSA's Acquisitions and Contracting Office, known as AQ, is profoundly and positively impacting the capability of AQ professionals to engage with stakeholders to successfully meet agency and customer mission requirements.

Moreover, AQ experts are proactive, inspired and enabled to provide the best acquisition and contracting services to support the agency's mission in each and every DCSA mission area – from personnel vetting, industry engagement, education and counterintelligence to insider threat support as the agency secures the trustworthiness of the U.S. government's workforce, the integrity of its cleared contractor support and the uncompromised nature of its technologies, services and supply chains.

"Our acquisitions and contracting team are establishing and building shared commitments with the mission area leaders and experts who are at the table with us," said Scott Stallsmith, DCSA AQ senior procurement executive, regarding the renewed focus that the AQ is creating on client engagement. "We will protect and prioritize customers' long term interests from a place of unique knowledge and professional duty."

Stallsmith, who joined DCSA in June 2021, outlined his five priorities for fiscal year 2022 and explained his goals for each of the following priorities.

• Invest in AQ employees

"By investing in our people, we will be able to create the workforce of the future, address critical skills gaps, improve productivity, drive future innovation and be the subject matter experts in our field."

• Hire, Onboard and Retain the Best and Brightest

"As we establish recruitment, retention and hiring best practices, we will be able to hire, onboard and retain the best and brightest."

• Make AQ a Center of Excellence

"By making AQ a center of excellence, we will be able to ensure the agency views AQ as the go to shop for contracting knowledge, advice – an office that can find solutions to their problems."

• Renewed Focus on Client Engagement

"We are creating a renewed focus on client engagement to protect and prioritize customers' long term interests from a place of unique knowledge and professional duty in addition to building shared commitments with each DCSA mission area."

• Support Governance Reform

"By supporting governance reform, we will be able to support enterprise boards and help them to succeed. Moreover, we will help them be a champion as they turn out quality decisions and documents."

A cornerstone for all of these initiatives is the AQ Integration Office, which leads AQ efforts for hiring, budgeting, workforce development, logistics and organizational development – all of which are vital to continue changes in order to meet the needs of DCSA's mission.

"While there have been many changes over the past two years in our Acquisition and Contracting Office, one thing that has not changed is our dedication to duty and doing whatever it takes to ensure that the DCSA mission is achieved," said Stallsmith. "Since AQ's inception, our contracting and support staff have executed more than 840 contract actions valued at more than $1.5B in support of DCSA mission needs. As AQ grows internally and implements new initiatives, we will continue to provide excellent customer service to continue meeting the needs of the DCSA mission."

AQ's expansion includes a new, fourth contracting office and is in the process of reorganizing the structure of each contracting office to provide the best support for their customers now and in the future.

> While there have been many changes over the past two years in our Acquisition and Contracting Office, one thing that has not changed is our dedication to duty and doing whatever it takes to ensure that the DCSA mission is achieved
>
> *~ Mr. Stallsmith*

Additionally, AQ continues to support a special project branch dedicated to the fieldwork services contract requirement of background investigations field operations in addition to the Enterprise Purchasing Branch in support of DCSA organizations that don't have their own government purchase card. What's more, AQ will add four senior contract specialists to serve as warranted contracting officers to alleviate workload pressure and chokepoints.

AQ has also established the Contracts Planning and Research (CP&R) Office to ensure compliance with DOD Instruction 4000.19 (Support Agreements) and the management of service agreements. The new CP&R Office supports the administration and promotion of the support agreement program, serves as the innovation cell and performs competition advocate duties among other functions.

This new capability will promote transparency within the acquisition and contracting process, enabling the agency to have a holistic view of all DCSA contract spend, whether that spend is a result of contracts with industry or as a result of inter-service or intra-service support by another DOD or federal agency.

To execute these responsibilities, a DCSA service agreements manager and components lead agreements manager have been designated with the responsibility of approving interagency agreements and engaging with customers in the planning, coordination and establishment of goals and milestones to ensure support agreement program success.

The Acquisition Management and Strategy team – comprised of the AQ Program Management Office, Policy and Oversight, and Systems and Data and Reporting – have been executing acquisition reform and governance initiatives in support of DCSA. As a result, AQ has implemented the Contract and Agreement Review Board (CARB), which provides oversight and adherence to best contracting practices. It ensures contract-related risks are discussed and mitigated and confirms that the contract strategy demonstrates sound business judgement while compliant with all statutes, regulations and policies.

The CARB is designed to reduce the procurement administrative lead time for DCSA acquisitions while strengthening oversight and the use of best business practices.

This is achieved through efficiencies gained in consolidating reviews of contract packages at the planning, pre-award and post-award phases. At each of these important milestones, contract requirements packages are reviewed by DCSA subject matter experts, including the Chief Strategy Office (CSO), the Office of General Counsel, the Small Business Program Office, the Office of the Chief Financial Officer, and the AQ Policy and Oversight Office as well as the head of the Contracting Activity and senior procurement executive.

Consequently, the new CARB eliminates the legacy linear process for the approval of requirements documents as they mature through the contracting process, saving time and resources in furtherance of the DCSA mission.

In order to further strengthen the DCSA acquisition model and provide more transparency to the acquisition process, AQ partnered with the CSO to assess the organization's acquisition governance. During the assessment, the working group concluded that while DCSA is generally compliant with DOD Instruction 5000.74 (Defense Acquisition of Services), improvements were required to be fully compliant while optimizing DCSA spend and further leverage the agency's buying power. To accomplish this, the AQ and CSO working group recommended several initiatives – two of which are the CARB and the establishment and appointment of a DCSA Service Agreements Manager.

CDSE CONVERTS INSTRUCTOR-LED COURSES TO VIRTUAL INSTRUCTOR-LED COURSES DURING PANDEMIC

By Samantha Dambach and Ian Bailey
Center for Development of Security Excellence

The COVID-19 pandemic created a need for social distancing, which presented a challenge for students requiring instructor-led training (ILT). ILT courses are taught in-person by internal and external (e.g., guest instructors, speakers) training staff at the Center for Development of Security Excellence (CDSE) in Linthicum, Md., and at various mobile training sites. Before the pandemic, CDSE offered both in-person and virtual courses; however most of its in-person content was not available in a virtual format. As a result of the pandemic, more virtual course offerings were needed.

CDSE evolved its offerings to serve security personnel by converting instructor-led courses to the virtual instructor-led training (VILT) platform, with the goal of having a virtual option for the in-person training. This effort sometimes presented IT technical and equipment challenges for some students, as they are employed with departments and agencies across the Federal Government. To mitigate these challenges, CDSE developed a quick IT requirements checklist, which is provided to students prior to course attendance. This checklist allows students to pre-coordinate with their respective organizations to ensure streamlined access and to help eliminate any organization specific technical difficulties prior to course attendance.

CDSE used several different delivery platforms to ensure students received the same training that was available before the pandemic. This included webinars via Adobe Connect to allow for instruction and student presentations. Additionally, in an effort to consolidate all CDSE courses onto a single platform, CDSE began migrating its courses to its Security Training, Education, and Professionalization Portal (STEPP). CDSE is completing this migration in a manner to maximize opportunity for students by maintaining its VILT courses without a break in service.

This response by CDSE to the global pandemic has allowed students to receive the attention and interaction of an in-person course from their home or office while continuing to develop security skills.

CDSE's instruction had a positive impact on security readiness across the U.S. Government by consistently providing an outlet for safe and impactful training during an environment where many training institutions struggled to deliver content. The virtual courses not only provided a way to continue training throughout the pandemic but also allowed the security community and cleared industry to save money that would be spent on travel.

During fiscal year 2021, CDSE delivered 56 VILT course iterations that resulted in 1,032 student completions during the pandemic. This is an increase from our prior average of 36 VILT course iterations delivered and 341 student completions. Moving forward, CDSE will continue to enhance its course offerings to further support the security community.

Student Feedback:

Intro to SAP-

"I had been trying to attend this class multiple times over the years and completing it at home was beneficial to me and family during the pandemic."

"Instructors did a great job at making themselves available for students. There was ample opportunity to ask questions and receive feedback on our work. The expectations and schedule/work load were well constructed and explained."

DOD SSC-

"I would have to say I took away several "nuggets" of useful information from every module, practical exercise and job aid….my "tool box" has grown significantly. The walk thru, step by step examples of the Risk Management Model helped me fully understand the logical process for what to protect and how to protect it, great framework. Also, the derivative classification exercise was challenging and really drove home the use of Security Classification Guides and originally classified documents to properly mark a document. I had a lot of questions and received timely replies from the staff to help make me successful in the course."

"Aloha, this course was a long time coming for me and I have to say that it was a great learning environment and I do appreciate the fact that we could complete this course on-line and in the comfort of my home. The course provided me a lot of information in the different security areas namely the industrial security program. The practical exams were good and gave me a sense of understanding each discipline and how it incorporates into each program. These last four weeks have gone by pretty fast but a lot was covered in the short amount of time we had. Completing this course has given me more knowledge and more tools for me in becoming more proficient within my career path."

The following courses are delivered in the VILT format

- Advanced National Security Adjudications
- DOD Security Specialist Course (SSC)
- Fundamentals of National Security Adjudications
- Getting Started Seminar for New Facility Security Officers (FSOs)
- Introduction to Special Access Programs (SAPs)
- SAP Mid-Level Management Course
- Physical Security and Asset Protection (PSaAP) (coming soon) **

GIST COMMITTEE WORKING TO ENHANCE AVAILABILITY OF SECURITY PRODUCTS

By Jason Steinour
Center for Development of Security Excellence

The Defense Counterintelligence and Security Agency (DCSA) Training Directorate is leading an extensive effort to enhance stakeholder engagement in the development and maintenance of security training products for the industrial security community. In fiscal year 2020 (FY20), the Center for Development of Security Excellence (CDSE) established the Government and Industry Security Training (GIST) Committee, which consists of two working groups. The first group was created specifically for government stakeholders in mind. The second group is a mixture of National Industrial Security Program Policy Advisory Committee (NISPPAC) industry stakeholders and DCSA representatives. The overall goal of the GIST Committee working groups is to enhance the availability of security products and services and foster a proactive, risk-focused culture.

GIST Committee participants are charged with evaluating policy changes and updates that impact the National Industrial Security Program (NISP), identifying existing and emerging training needs, discussing the development of relevant and innovative content and services that support security awareness, and expanding the delivery of security training products and services. These meetings occur virtually on a quarterly basis through Adobe Connect. This virtual platform offers an open forum for stakeholders to discuss existing products and provide recommendations for improvement, while simultaneously discussing ideas and recommendations for new product development based on current training needs and policy. Poll questions and open chat pods are some of the techniques meeting facilitators use to obtain feedback and recommendations from working group participants.

In FY20, both working groups received a summary of a training needs analysis, which provided information on existing CDSE training products, stakeholder needs, policy requirements, and suggestions for new product development. In FY21, both groups provided feedback which assisted in the maintenance and development of additional products made available to the industrial security community. Successive meetings focused on certain policies and procedures that required

additional training and development of new products to meet these needs. Participants reviewed product development ideas and product development prototypes. Their active participation resulted in the design and development of several new products, and the development of the overall content areas and policy requirements for these new products. All industrial security training products developed during the initial stages of these working groups eventually received a full vetting through these working groups.

GIST Committee members' participation resulted in:

Revised products

A complete revision of the virtual instructor-led course Getting Started Seminar for New FSOs, maintenance of the Industrial Security for Senior Management and *You're a New FSO: Now What?* shorts, NISPOM Reporting Requirements and Annual Planner job aids, and several eLearning courses.

New products

CDSE also created new products based on GIST Committee feedback including several National Access Elsewhere Security Oversight Center webinars, Understanding the DCSA Security Review and Rating Process and Industrial Security Policy Changes webinars, Insider Threat Overview for FSOs and Maintaining an Effective Industrial Security Program security training videos, an Industrial Security Comprehensive Glossary job aid, and several security posters.

Our committee members assisted in the maintenance and development of training products by discussing policy and procedure changes, recommending ways to address training needs, sharing feedback on proposed content and structure of training products, and vetting the final product prior to its release. The collaborative efforts between government, industry, and DCSA representatives resulted in enhancements to new and existing products available to the NISP community. Going forward, CDSE will continue to engage actively with stakeholders through the GIST Committee working group meetings to openly discuss policy, training needs, and product development.

DCSA BY THE NUMBERS

Each year it's a tradition to look back and get a sense of what has been accomplished. DCSA is no different. The following is a look at the agency and its accomplishments:

AGENCY:

10,000+ employees & contractors
167 field locations
$2.433B – DCSA FY22 budget
- Working Capital Fund- **$1.302 billion**
- Appropriated Funds- **$1.130 billion**

BACKGROUND INVESTIGATIONS:

2.2 million Investigations completed
18 million Investigative items closed
19% Reduction in inventory, decreasing by **41,000**
Achieved **74** days to complete Top Secret cases during 3rd Quarter
53 days Secret/Confidential (T3) investigations
2,800 cases prioritized in support of Health and Human Services Unaccompanied Refugee Minors Program

ADJUDICATIONS:

824,326 Cases closed
11 days National Security Initial timeliness (annual)
31 days National Security Reinvestigations timeliness (annual)

VETTING RISK OPERATIONS:

1 million National Industrial Security Program (NISP) contractors with clearance eligibility

Continuous Vetting:

3.6 million enrolled
495,000 CV enrollees with deferred periodic reinvestigations
30 Agencies enrolled in TW 1.25 service

Expedited Screening:

127,000 – Initial T3/T5 background investigations screened
28,000 – International Military Students screened

INDUSTRIAL SECURITY DIRECTORATE:

5,773 Continuous Monitoring Engagements
4,033 Security vulnerabilities identified
1,154 Facility clearances issued
1,129 Security violations processed

NISP Authorization Office:

6,174 NISP classified systems
3,490 Authorizations issued

International:

2,237 Outgoing requests for visits
8,208 Traveler/visitors

Arms, Ammunitions and Explosives:

24 Inspections completed

THREAT DIRECTORATE:

Office of Counterintelligence (OCI):

23,906 Reports of suspicious contact from industry

555 Referrals to Law Enforcement/Intelligence Community

140 Investigations/operations opened due to Threat Directorate referrals

2,878 Intelligence information reports

OCI Cyber:

374 Specific Cyber Threat Alerts

DOD Insider Threat Management and Analysis Center:

2,842 reports submitted to the DITMAC

1,154 Reports from components based on Continuous Evaluation alerts

11 Department of Justice referrals for unauthorized disclosure (UD) of CNSI and CUI

TRAINING DIRECTORATE:

Center for Development of Security Excellence:

4,744,142 Course completions

9,240 Active certifications

1,476 Conferrals in SPēD Certification Program

121 Advanced Level Education course completions (16 Weeks)

National Center for Credibility Assessment:

43 Course completions

1,621 attendees

Defense Counterintelligence and Security Agency

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