TOGETHER,
WE ARE
AMERICA'S

Gatekeeper

Official Magazine of the
Defense Counterintelligence and Security Agency

Volume 1, Issue 1

IN THIS ISSUE

IN THIS ISSUE

VOL 1 | ISSUE 1

DCSA Gatekeeper

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

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil
571-305-6562

DCSA LEADERSHIP

William K. Lietzau
Director

Troy Littles
Chief Operating Officer

Jon Eskelsen
Chief, OCCA

Cindy McGovern
Managing Editor

Elizabeth Alber
Editor

Christopher P. Gillis
Staff Writer

Becky Moran
Cady Susswein
Jason Shamberger
Kara Ewell
Andrea Ploch
Ryan King
Monika Thomas
BARBARICUM
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

You will notice a major change to this publication — it is no longer the ACCESS. Today, our flagship publication has become the Gatekeeper, and we have kicked it off as Issue 1 of Volume 1. Why have we done this?

I made this decision to better reflect the fundamental transformation that has taken place. We are a new agency. As a technical matter, the Defense Security Service's name was changed and then took on many other organizations, personnel, missions, and resources. But most readers are well aware that a simple renaming and shifting of office locations does not sufficiently capture the gravity of transformative change that yielded what is essentially a new agency — the Defense Counterintelligence and Security Agency, or DCSA.

The creation of this new agency has had, at its heart, two distinct transfer phases. The largest occurred on October 1, 2019, when three organizations merged: the Defense Security Service (DSS), the Office of Personnel Management's National Background Investigation Bureau (NBIB), and the Department of Defense's Consolidated Adjudications Facility (DoD CAF) came together to form DCSA as the largest security organization in the U.S. government. Together, we represent the nation's largest background investigation service provider, the nation's largest suitability, security clearance, and credentialing provider, and the largest industrial security credentialing organization. This merger included over 4,000 government employees, 9,000 contractors, and 167 facilities and field locations.

On October 1, 2020, we completed the second phase of transfers. Although involving smaller offices and organizations, this transfer phase was equally complex and significant. It involved sensitive mission, function, and system transfers from the Defense Information Systems Agency (DISA), Defense Manpower Data Center (DMDC), Defense Intelligence Agency (DIA), and Office of Personnel Management (OPM). Through this phase, DCSA was supplemented with approximately 150 government employees, 500 contractors, and 14 information technology systems.

So why change the name of this publication? ACCESS Magazine was started and faithfully produced by DSS for 10 years. Every employee who came to DCSA from a predecessor organization has reason to be proud of their previous work, but we are not DSS anymore, nor are we NBIB, OPM, DISA, or any of the other antecedent organizations. The hard work of every employee at DCSA, coupled with the efforts of many outside the agency, have yielded a new agency, built to meet the needs of a new era — one in which each of our functions has never before been more important, our missions have never been more complex, and the price of failure has never been so high. It only stands to reason that we would have a new magazine that is not merely an evolved version of a previous mission area's publication, but one that reflects the totality of our new mission set. DCSA's Office of Communications and Congressional Affairs (OCCA) conducted two employee surveys to identify a name for the new agency's publication, and "Gatekeeper" was the overwhelming favorite. The fact that it happens to reflect our mission statement is not coincidental — it truly reflects our national security role.

Our individual histories and legacies helped to define who we are today. Our mission, vision, and values as a new agency will define us into the future. The articles you will see in the pages of this publication reflect that future. You will find an article on DCSA's Operating Model — how we intend to leverage sometimes disparate functional areas to form a holistic, comprehensive security view of personnel, facilities, industry entities, and systems. You will also see an article on the National Background Investigation Services (NBIS) — the next-generation IT system that will serve as the backbone of the investigative mission, ultimately replacing antiquated legacy systems. Both of these initiatives are forward-focused and will underpin the agency's work for years to come.

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

William K Lietzau

William K. Lietzau

Director,
Defense Counterintelligence
and Security Agency

ASK THE LEADERSHIP

DAVID STAPLETON

ASSISTANT DIRECTOR, CRITICAL TECHNOLOGY PROTECTION

Editor's note: In each issue of the Gatekeeper, we feature an interview with a senior leader on their background, mission, and program priorities. David Stapleton, who joined DCSA in June 2020, serves as the assistant director for Critical Technology Protection. Critical Technology Protection is one of the director's top priorities, and Stapleton brings a unique perspective to the position.

Stapleton most recently served as the director of trusted capital, a program launched within the Department of Defense (DoD) to combat adversarial capital — the threat of deliberate foreign investment in nascent and potentially sensitive U.S. national security technologies — and build a trusted capital marketplace that offers trusted capital providers the opportunity to invest in key DoD focus areas. Previously, he served as the acting deputy assistant secretary of industrial policy, where he initiated five Title III Defense Production Act programs. These programs mobilized purchase commitment authority to build revenue for critical companies, assisted the Committee on Foreign Investment in the U.S. (CFIUS) in bringing U.S. technology transfers with adversaries to historic lows, and created the Trusted Capital program. From October 2016 to 2019, he also led Global Markets and Investments, where he served as the DoD lead for CFIUS.

Stapleton began his career on Wall Street, where he last served as vice president and group head of market strategy at JPMorgan. Following the terrorist attacks of September 11, 2001, he left Wall Street for the U.S. Marine Corps, where he commanded a Marine sniper platoon in Afghanistan, a reconnaissance platoon in Iraq, and a reserve force recon unit.

He remains in the Marine reserves, where he most recently served as commanding officer of the 4th Recon Battalion. Prior to joining DoD as a civilian, he was an adjunct instructor in political science and economics at the U.S. Naval Academy and served for three years as the chief operating officer of a startup tech company.

He earned an M.A. in international relations from Columbia University, an Executive M.B.A. from the Wharton School of the University of Pennsylvania, and an accelerated J.D. from Northwestern University. His Bachelor's degree is in political science from Georgetown University.

Q: We have your biography, but what do you want people who read this to know about you?

A: I have no price tag. I was born and raised in a small steel and prison town where many of the blue collar jobs in industry went out of business in the 1970s. But, that community had tremendous values and principles that remain to this day. The people there cared about what you did for the community and the nation. They wanted to know if you worked hard, earned an honest living, and kept your word. That family and community upbringing has always guided my life and my commitment to service both in the government and the Marine Corps. I am fighting for the small town industries that are the heart and soul of our nation and against an adversary who is hell bent on the destruction of those industries and the free world.

Q: You came to DCSA from the acquisition community. Do you think that experience will help you in your current position?

A: I think it has definitely been helpful and given me a perspective on the need for a holistic approach to national security. I can see the need, from the acquisition side, to be able to incentivize industry to do the right thing. The protection of their revenue is critical in this dynamic, and we have to synchronize that with security. We also have to offer solutions to the acquisition community that are running fast, while working with companies that are secure. We have to look at the issue through industry's lens and their long-term viability and profitability, which includes ensuring they are protecting their intellectual property and the sensitive and classified information that is unique to that business.

Q: You are now seeing acquisition and security from the other side so to speak. What have you learned since arriving that you didn't expect or is different from your previous experience?

A: Given our forward position with industry in the field, DCSA is uniquely positioned to operationalize solutions. Just as with the acquisition community, solutions are predicated on systems that can help augment the field agents in their daily responsibilities.

Q: The 2018 National Defense Strategy states: "Maintaining the Department's technological advantage will require changes to industry culture." What is CTP doing to affect culture change within industry? How do you view the agency's relationship with industry?

A: We are seeing threats to industry that include the full spectrum of economic warfare. As a result, we have to partner with industry to help them internalize capabilities that not only protect them and their intellectual property, but also the nation. Industry has to see what's in it for them. They have to see security as a protection of a valued revenue stream for increased research and development — and profits — rather than a cost center that negatively impacts their bottom line. The United States is losing $200 to $600 billion per year to our adversaries. We should all be aligned in that partnership and in raising the standards together. DCSA is working with industry to ensure that they are holding themselves to the standards that will protect their intermediate and long-term profits, alongside our nation's defense industrial base.

Q: Within the past few years, DCSA was very focused on moving from NISPOM compliance to a risk-based approach to industry oversight. Can you talk about this initiative and next steps?

A: A risk-based approach to what we do is really about addressing the protection of national security for both ourselves and industry in a way that is scalable across the program. It is also about adopting the best systems and analytics to enable that functionality in concert with our industry partners. The NISPOM — National Industrial Security Program Operating Manual — is a basic framework for security that guides industry. At the same time, we should internalize and adapt to today's ongoing, highly adaptive threats from our adversaries. The challenge is finding that balance and implementing it.

Q: The threat of foreign influence is greater than ever. What is CTP doing to assist industry in mitigating the threat of foreign influence, and how do you see this changing in the future?

A: We have to help industry understand economic warfare and provide them with the tools to fight our adversaries. It is essential to our mission, and we are developing a host of new capabilities to address this. For instance, we are looking at a risk-based framework that can be adaptive to our adversaries and protect the companies that are going up against countries. Industry has seen the opportunity to work with non-market economies, and we have seen how that has undermined the capability to share in a global economy. We have a different perspective on where we can learn from our mistakes and help others prevent future losses of information vital to national security.

Q: What do you see as the biggest challenge facing CTP?

A: Typically, most solutions within the U.S. government involve applying more human capital to a solution. We are focused on leveraging systems and processes that can augment human capability to improve our support to industry as well as internal production. We are working toward a common operating picture that leverages data analytic tools across the agency to develop that picture for industry, DCSA, and across the Department of Defense.

Q: The field is where the day-to-day interactions with industry occur. What message do you have for them? What can they expect under your leadership?

A: Our field workforce is the heart and soul of our operation. They are the frontline operators in economic warfare. Their support to cleared industry, and recently Operation Warp Speed, is vital to both the immediate and long-term success of our mission. From a leadership perspective, I want everyone to know that we need one another internally and externally. No one will win this fight alone, but one company or person alone can lose this fight. We do not tolerate a different standard across different companies. We cannot dilute the standard for a company at the expense of national security. Regardless of what relationship or title people have held, they should expect application of the same standard, and that is what industry should also demand from us. Many of the senior leaders who engage with DCSA once served in federal government and would not have wanted us to change a standard on their watch in government, so it should be no different when they are with industry.

THE FUTURE PERSONNEL VETTING IT SYSTEM

Since 1985, the federal government has amassed 85 Information Technology (IT) systems supporting the background investigation process. Thousands of security professionals access these systems daily, often jumping from platform to platform to initiate, monitor, and manage countless personnel security actions. At the same time, each of these systems needs to be individually sustained and protected against adversarial attacks and unwitting spillages. The OPM data breach in 2015 proved that a solution not only to better protect data but to streamline the process and reduce the access points and time needed to conduct high-quality background investigations was of immediate importance.

The Department of Defense (DoD), with the Defense Information Security Agency (DISA) at the helm, embarked on a journey to deliver a solution to bring these disparate systems into one modern federal personnel vetting IT system. On Oct. 1, 2020, DCSA took on the mission to finish building and ultimately implement the department's solution, known as the National Background Investigation Services (NBIS).

NBIS includes all steps of the background investigation process from the initiation and application stages to investigation, adjudication, and continuous vetting. It will build upon and replace the legacy background investigation IT systems over time, ultimately serving as the one-stop shop for the entire personnel vetting process. By consolidating the legacy IT requirements, NBIS offers an end-to-end capability, providing users an effective, secure, and efficient environment, while allowing DoD to implement upcoming policy reforms to personnel vetting.

INITIATION

Position Designation Tool

APPLICATION

Electronic Questionnaire for Investigation Processing (e-QIP)

Secure Web Fingerprint Transmission (SWFT)

Fingerprint Transaction System (FTS)

INVESTIGATION

Individual Investigation Records Repository (IIRR)

Defense Central Index of Investigation (DCII)

Field Work System (FWS)

Non-Field Work System (FWS)

Personnel Investigations Processing Systems (PIPS)

OPM PIPS Imaging System (OPIS)

ADJUDICATION

Case Adjudication Tracking System (CATS)

Joint Verification System (JVS)

Joint Personnel Adjudication System (JPAS)

Central Verification System (CVS)

CONTINUOUS VETTING

MIRADOR

> **"We accept this no-fail mission."**
> —William K. Lietzau, DCSA Director

"We accept this no-fail mission," said DCSA Director William K. Lietzau. "As America's gatekeeper, maintaining the security of our data and innovating ways to streamline the personnel vetting process are essential to protecting our nation's trusted workforce. NBIS will improve the speed and quality of the background investigation process by modernizing our IT infrastructure and taking it into the 21st century."

NBIS is designed to deliver more robust security, additional customizable solutions, and faster processing, while also enhancing users experience.

Integrated: With one consolidated system, security managers, investigators, and adjudicators will now be able to access case status from a single platform throughout the lifecycle of a background investigation, enhancing capacity and creating synergies through easier data validation.

Continuous Improvement: NBIS is leveraging proven Agile and Development Security Operations (DevSecOps) pipeline approaches to software development to speed up delivery, improve functionality, deliver more customizable solutions, and further enhance security. This approach will facilitate easier upgrades that do not require an entire system overhaul.

Faster: New features such as e-Adjudication and mass initiation (allowing users to request investigations for multiple similar subjects at once) will greatly expedite the investigation process. Security managers will also be able to tag cases and develop refined metrics that meet their reporting needs.

Continuous Vetting: NBIS will functionalize new innovations to the background investigation process such as continuous vetting, which will allow DCSA to move from periodic reinvestigations to real-time automated record checks that immediately alert investigators of a threat. These automated record checks cover seven data categories: Terrorism, Foreign Travel, Suspicious Financial Activity, Criminal Activity, Credit, Public Records, and Eligibility. There are currently 2.3 million cleared DoD personnel enrolled in four of seven data categories with a requirement to grow the entire DoD cleared population (approximately 3.6 million) in all seven data categories.

A Streamlined Questionnaire for Applicants: The new eApp will replace the Electronic Questionnaires for Investigations Processing (e-QIP). eApp improves the background investigations experience for clearance seekers by addressing the most challenging part of the process — the questionnaire. New features will cut down the number of agency reviewer kick-backs and late stage corrections, simplifying and speeding up the entire process.

More Secure: NBIS will be housed in an encrypted cloud environment with multiple layers of protection. It is a secure system that was designed to compartmentalize sensitive data so that large amount of data cannot be compromised in the event of an attack.

NBIS PRIORITY: DATA AND SYSTEM SECURITY

NBIS delivers multiple layers of security with end-to-end data encryption, isolation, and filtering to compartmentalize sensitive information and prevent large data spills in the event of an attack.

The early stages of NBIS capabilities have already begun rolling out. A position designation tool to establish the risk level for sensitive government positions has already been integrated into NBIS, and eApp is now available for certain segments of the population filling out the Standard Form 86 (SF-86) only. NBIS is expected to continue to roll out incrementally, providing new and improved capabilities as they become available.

EAPP BENEFITS

Address Checks

A new address check function leverages the U.S. Postal Service address validation tool to verify address accuracy.

Timeline Validation

eApp will now alert applicants if there are gaps in required timelines, such as breaks in work history.

Real-time Feedback

Real-time feedback alerts applicants to discrepancies as the data is entered, such as entering a document expiration date that occurs before the issue date.

Section Reviews

Applicants can now correct errors, such as missing data fields, directly on the review page at the end of each section.

Help Section

A new help section provides definitions, clarifies acronyms, and simplifies directions.

Section Reordering

eApp reorganizes each questionnaire section into more intuitive and logical groupings.

Question Branching

Follow up questions and sub-sections will only appear if necessary, based on the applicant's answers.

Mobile-Responsive Layout

Now mobile responsive, eApp can be more easily viewed on tablets and smart phones.

Auto Saving

eApp autosaves applicant progress if applicants need to leave a page.

eApp new and improved features will accelerate the background investigation process by improving the way applicants submit and verify information.

> **"Our goal with NBIS is to deliver secure and quality IT solutions, while minimizing disruptions for our customers."**
>
> —Terry Carpenter, DCSA Program Executive Office

"Our goal with NBIS is to deliver secure and quality IT solutions, while minimizing disruptions for our customers," said Terry Carpenter, DCSA Program Executive Office. "We want to expedite the path to operational background investigation and continuous evaluation capabilities, but not at the expense of current operations. We are closely monitoring the implementation, enrollment, and adoption rates at each step along the way to ensure a high-quality customer experience."

Technology and cyber threats are always evolving. NBIS is the department's solution to match the pace, leveraging cutting-edge technologies to improve delivery and protection of our trusted products and services.

DCSA OPERATING MODEL: UNITING THE AGENCY IN ACHIEVING ITS VISION

By Nicoletta Giordani
Chief Strategy Officer

SETTING THE STAGE: WHY IMPLEMENT A NEW OPERATING MODEL

When the president signed Executive Order (EO) 13869, "Transferring Responsibility for Background Investigations to the Department of Defense," several organizations merged into DCSA. However, the task of translating this EO into reality had only just begun. DCSA components are currently still operating similarly as they did before EO 13869. That is, in silos, where DCSA's Personnel Vetting, Industrial Security, Counterintelligence, and Security Education and Training missions are conducted largely independently. Some collaboration is happening today, and pockets of even more are emerging, but there has been no enterprise-wide model that formally standardizes the cross-component collaboration needed to truly fulfill the agency's core purpose — to serve as the nation's preeminent security organization.

The Chief Strategy Office (CSO), in collaboration with DCSA mission areas, is working to change that with the introduction of the agency's new Operating Model (OpModel). This OpModel will define how core missions and supporting operations come together to optimize mission performance and customer service through increased use of risk-management approaches, empowerment through technology and data, and the scaling of enabling support to meet evolving mission needs. The agency is looking to the future and prioritizing how resources can be best leveraged to operate as one enterprise to accomplish its mission. The OpModel will serve as a guide over the next few years to achieve the agency's vision.

WHAT IS AN OPERATING MODEL?

An OpModel is not an organizational chart, process map, governance charter, or cost-cutting plan. Instead, it is a clear articulation of how an organization's capabilities come together to perform work and deliver mission value. As a new agency responsible for a complex mission set, DCSA is directly affected by many external changes, including new policies, new technologies, and an ever-changing threat landscape that directly impacts our missions.

Opportunities for Cross-Mission Collaboration

DCSA conducts both facility clearance (FCL) and personnel clearance (PCL) investigations. The OpModel will standardize the collaboration required to attain, analyze, and share vast amounts of data to identify trends and best understand risks across these missions. The PCL data on personnel comprising a given facility can ultimately help inform the risk that facility presents, thus help DCSA make more informed decisions on FCL determinations and better understand general security risks and potential threats.

These conditions require DCSA to approach emerging challenges and opportunities more holistically to meet mission needs. The OpModel provides the enabling guidance to achieve this by serving as a "north star" for how DCSA operations must transform. For example, in the face of an ever-changing threat environment, an OpModel can help by laying out a deliberate, methodical approach to promote the alignment of resources, personnel, priorities, and organizational structures to meet mission challenges.

DEVELOPING AN OPERATING MODEL THAT BEST SERVES DCSA

The development of a DCSA OpModel has been underway for the past year, starting under the Personnel Vetting Transformation Office (PVTO) in October 2019 and transferring to DCSA with the stand-up of the CSO. Central to this effort is engagement with the mission leaders and experts at each step in the OpModel's development. The CSO began developing this concept by deploying a three-phased approach:

- ***Discover*** the current state of how DCSA operates,
- ***Diagnose*** the pain points and opportunities related to improving mission performance, and
- ***Design*** a path to address the pain points and accelerate the opportunities.

The OpModel Seeks To:

- Position the agency for optimized performance — ensuring fluid coordination and integration between missions across DCSA and in the field, while increasing knowledge-sharing, transparency, and accountability.
- Integrate data sources and risk indicators into operations to drive risk-based and data-driven mission decision-making across mission areas and their field counterparts.
- Enhance how DCSA delivers the customer experience and enable the agency to become more customer-centric.
- Equip DCSA personnel with modern technology, scaled across the agency, to optimize the capacity for field operations and those onsite to provide efficient mission delivery and adapt to future changes and threats.
- Replace ad hoc services with standard delivery through routine processes and clear governance for enabling support services to the mission leadership and workforces across the agency.
- Contain costs and allocate resources toward mission delivery and strategic investments to improve mission performance.

In the **Discover Phase**, the OpModel team conducted over 60 interviews with DCSA leaders, external partners, and personnel (e.g., mission experts and field agents) to baseline the current state of operations across DCSA. To gain an understanding of the pain points for the field workforce, the team launched a FieldBot survey that yielded an 80% return rate, providing insight into the operational and integration needs for the majority of our workforce — the field. In addition, the team conducted interviews with the leadership teams for five of the enabling support offices providing services to DCSA's missions — the Office of the Chief Information Officer (OCIO), Office of the Chief Financial Officer, Human Capital Management Office (HCMO), Acquisition, and Logistics Management Division (LMD).

Based on these inputs, industry research, and federal best practices, the **Diagnose Phase** identified key focus areas to design the most impactful approach to improve mission performance both in the field and across mission areas, with an emphasis on several focus areas: threat coordination, industrial security risk management, continuous vetting maturation, customer alignment, field integration, and enabling support.

In the **Design Phase**, the team collaborated with mission experts in focus groups to develop viable courses of action and process changes to mature these mission capabilities and inform the overall enterprise OpModel design. The recommendations from each of these focus groups, two visioning sessions, and additional refinement through targeted engagement with mission owners informed an overarching design concept. This concept will serve as the basis for transformation and provide a common operating picture of how DCSA delivers its value to customers.

The implementation of the OpModel aligns with the DCSA director's strategic goals to drive DCSA transformation over the next few years. This graphic depicts the director's strategic goals and the focus areas set forth to achieve them:

STRATEGIC GOALS

1	2	3	4	5
Transform mission performance to reduce risk and improve operational outcomes	Create world-class customer and mission support capabilities	Use technology to modernize operations and drive innovation	Optimize the use of data to improve mission and business effectiveness	Align requirements and resources to agency priorities

TRANSFORMATION FOCUS AREAS

• Core Mission Optimization • Field Integration/ Process Improvement • Change Management/ Strategic Communications	• Financial Management Transformation • Enterprise Service Delivery • Customer Experience	• IT Strategy and Roadmap • R&I Portfolio Management	• Data Strategy and Management • Performing Measures and Reporting • Predictive Analytics • Knowledge Management	• Enterprise Governance • Requirements Management

The first two goals will be realized through the implementation of OpModel recommendations in six transformation focus areas—core mission optimization, field integration, financial management transformation, enterprise service delivery, customer experience, and the stand-up of a change management capability to facilitate OpModel implementation. The other three goals both complement and directly support the implementation of OpModel recommendations through the intentional application of technology, data management, performance metrics, and governance. These transformation focus areas set the basis for DCSA to achieve the strategic goals, bringing the OpModel vision to life for the enterprise. Laying the firm foundation for early success will enable building a stronger operational framework for the future as DCSA transforms its capabilities and infrastructure.

COMING SOON: BRINGING THE OPMODEL TO LIFE

The CSO seeks to ensure that mission areas understand how the OpModel will benefit them and how their implementation will serve the enterprise and further national security. The actual shift to adopting the OpModel will be less disruptive than it might appear. OpModel implementation does not immediately lead to new organizational hierarchies or alter the chain of command. Instead, it presents a framework for how organizations must work together to achieve strategic goals. The CSO will continue to work closely with each part of DCSA, jointly planning implementation activities to maximize the efficiency and effectiveness of DCSA mission areas. Immediate next steps for most mission areas will be to conduct a readiness assessment of the proposed changes and define concepts of operations (CONOPS) that will codify how the proposed new approaches will come together across the missions with adherence to appropriate authorities and policies. This deliberate planning seeks to underscore DCSA leadership's commitment to collectively invest in reaching the agency's future state vision.

OpModel implementation will involve fully integrating technology and improving metrics management practices, making more data-driven decisions in an array of areas from field operations to resource management to acquisitions. Ultimately, the OpModel is only a concept. It will take the drive and commitment of all DCSA components to help apply this concept to maximize the agency's potential as the nation's preeminent security organization.

Engaging the Workforce

It is critical that the DCSA workforce has a shared understanding of the OpModel concept and how the OpModel will eventually impact work lives. For this reason, the CSO will launch an outreach campaign in January that includes a virtual "roadshow," with the CSO hosting webinars with mission areas and regional offices to deliver information on the OpModel and allow for questions and answers. The CSO will also hold virtual coffee chats — informal meetings where any DCSA employee may engage with DCSA leaders and ask questions about the OpModel and the future of DCSA.

The following articles are the latest installments of the "Day in the Life" feature, a series of interviews following members of the DCSA community and their daily roles in accomplishing the agency's diverse mission set.

Editor's Note: Some of the following interviews took place prior to the COVID-19 outbreak and may not reflect existing DCSA operations.

A DAY IN THE LIFE: INDUSTRIAL SECURITY

DCSA provides industrial security to nearly 10,000 cleared companies and 12,500 cleared facilities. DCSA has a diverse team helping to ensure industrial security measures are met through inspecting and monitoring companies. Find out more about these individuals and the roles they play within DCSA.

JOANNA MEMBRENO

Business Analyst, Foundational Analysis

Q: What does the business analysis unit do?

A: The Business Analysis Unit (BAU) assesses facilities in the National Industrial Security Program (NISP) for the existence of foreign ownership, control, or influence (FOCI) vulnerabilities and recommends strategies for mitigating risks to national security. We are a team of experts in security, acquisitions, intelligence, finance, corporate law, and corporate governance.

Within BAU, there are two teams: Foundational Analysis (FA) and Advanced Analysis (AA). While both look at a company from a FOCI standpoint, typically, when FA finds a foreign connection (such as foreign ownership), the AA shop will do a more extensive review. As a member of the FA shop, I perform a holistic review of a facility to find any FOCI concerns. I look at how the facility is aligned and organized at the corporate level and whether there are any risks to maintaining a clearance. My office will look at facilities applying for a first clearance as well as currently cleared companies that have undergone some sort of change, such as a shift in its organizational structure or change in ownership.

First, I look at a company's corporate documentation to get a better understanding of their operations. I analyze business structure and break it down to establish who owns it and who controls it. I look at its many different components, such as its governance, contracts, interactions, and revenue to discover potential vulnerabilities. For example, I will look at a facility and the way it's organized to handle foreign interactions to assess its ability to safeguard classified information. Our office uses self-reported information as well as open source research to do our due diligence on issues that may not have been openly conveyed.

We have a couple of different mitigation instruments and supplements in place to mitigate a facility's FOCI concern. It really depends on the degree of FOCI present at the facility or its parent company that will dictate the mitigation type. Mitigation can vary from a board resolution to a more stringent mitigation such as a proxy agreement.

Outside of FOCI assessments, our unit also writes National Interest Determination (NID) assessments and reaches out to external agencies — like the National Security Agency (NSA) and the Office of the Director of National Intelligence (ODNI) — to strengthen or establish FOCI programs, share information, and create partnerships. One of the most recent collaborations I participated in was with a BAU-equivalent office at the Department of Energy (DOE). The DOE reached out to us looking for insight on how we conduct business analysis as their administration of clearances is a bit different. Our work is slowly but surely becoming more widely recognized among other government partners.

Q: How do you collaborate across DCSA?

A: Our unit works hand-in-hand with the facility clearance branch and industrial security representatives across the country. The AA shop will also collaborate with the Counterintelligence (CI) directorate in the event we find any vulnerabilities that flag a set of risk-based indicators. We're a very niche group with a very niche mission. I need to consider so many elements, and to a certain extent, act as the fulcrum between the field element and other elements.

Q: What do you love about your job?

A: What I love about my job is the fact that our mission is so unique, and my team is so incredible. I like my team because it is comprised of individuals with a colorful array of experience and professional backgrounds. Because we are all so different, it's invigorating to learn from each other and see things from a different analyst's perspective. I've grown a lot looking at things through someone else's "analytical eye."

> *What I love about my job is the fact that our mission is so unique, and my team is so incredible.*

My work is difficult because of the level of scrutiny necessary to vet facilities. There are so many different scenarios I experience, there isn't ever a mundane day at work. I have a degree in business administration and marketing, and I still maintain that passion for business. I get extremely excited when I'm talking about business in general, especially when it comes to stock ownership — I find all of that fun. It's thrilling to be able to tie my business background with something new, like industrial security and government. I'm happy to be able to do what I love and do it for a greater good, rather than just for profit. There is a true purpose to what I do.

Q: How does the BAU fit into DCSA's mission?

A: We add the element of due diligence to the facility clearance process, which is essential in accomplishing the mission. For background investigations, investigators go and research information, which is one of the most important parts to granting someone a personal security clearance. For the industrial security side, I have a very similar role. My research and discovery help move forward the facility clearance process and supports the ongoing maintenance of companies that are already cleared within the NISP. As a continuous vetting element, it's important to monitor changes a company may undergo to ensure they don't adversely affect national security.

JEFF CAVANO

Senior Program Security Manager, International Special Access Programs Division

Q: What does a Senior Program Security Manager in ISAP do?

A: My job is to manage special access programs (SAPs) in the hands of industry. SAPs are designed to provide enhanced security measures to protect the United States' most critical and sensitive capabilities, technologies, information, and operations. To make sure that each contractor is meeting its security requirements, we work to ensure industrial security representatives (ISRs) are eligible, SAP-accessed, trained, and prepared to conduct SAP security inspections. We provide them with outreach briefings on SAP process, procedural and policy changes, and reporting updates to ensure they have the necessary tools to conduct SAP inspections.

We also work directly with the government contracting agencies (GCA) that contract with industry to produce the sensitive or critical technology and program security officers to make sure we understand and communicate their needs to ISRs that conduct SAP inspections at contractor sites. When an ISR submits an inspection report, we provide a quality assurance review to make sure the contracting agency's needs are met. Depending on the complexity of a situation, we also provide government oversight verifications of activities outside DCSA's security cognizance.

I also participate in the Arms, Ammunition, and Explosives (AA&E) working group. Part of the agency's responsibility is to assess the physical security of a facility before they are awarded a government contract. ISRs make sure the contractor has adequate security in place to protect and safeguard AA&E during its manufacture. If the contract is awarded, ISRs conduct

recurring onsite annual physical security inspections of AA&E facilities. Presently, we are working to centralize the oversight mission at headquarters in Quantico, Virginia.

Q: What are the most rewarding aspects of the job?

A: What I love about this job is my contribution to the Industrial Security mission. When I was on active duty, I deeply appreciated the technological advantages the U.S. military enjoyed, so I want to contribute in ensuring our military and technological advantage. As a civil servant, I've worked in critical technology protection my entire career — at Defense Transportation Security Agency (DTSA), the Joint Staff, and the Intelligence Community — but DCSA is truly where we multiply our impact. Our SAPs protect the most critical and sensitive capabilities and technologies in development, so that's what drew me in.

> *Every day, I learn something new working with and learning from SAP stakeholders, it's fulfilling work.*

I thoroughly enjoy working with the field agents that execute Industrial Security mission at the ground level. Every day, I learn something new working with and learning from SAP stakeholders, it's fulfilling work.

I'm also looking forward to seeing how DCSA changes the way we do business with the fusion of the Industrial Security, Personnel Vetting, and Counterintelligence missions. A synergistic approach, along with increased IT capabilities, may equip us to disrupt and degrade any future loss of our technological edge.

Q: What advice do you have for perspective employees interested in the field?

A: Study hard and learn from everyone. Every day I learn something that I didn't know I didn't know. The world is changing, and with critical technology protection, you have to toggle your attention between the strategic context and the nitty gritty details. Security can be a complicated business, but our folks in the field are doing fantastic work.

FRANK GRANDE

Information Systems Security Professional, Critical Technology Protection

Q: What does an ISSP do?

A: In short, I'm a cybersecurity specialist. I work with 112 facilities under the National Industrial Security Program (NISP) to mitigate any risks associated with their information systems. When a company applies for a facility clearance or I'm doing an annual assessment, I typically go out to the facility and do an onsite validation to ensure that the contractor is meeting NISP requirements in practice. I normally look at all the documentation the facility provides and give feedback like, "these controls look compliant" or "these don't." When a facility is non-compliant, I initiate a plan of action and milestones, basically a "get-well plan," in which facilities document what and when they are going to make the controls compliant.

For every network and computing system I oversee, there are between 1,380-1,420 controls that have to be manually inspected to ensure that the contractor is properly protected. Although these controls are documented and updated in eMASS — the Enterprise Mission Assurance Support Service — there's no automated control review. I have to manually look at each of them to ensure it's all compliant.

Once complete, I send the results to my team lead, who reviews the packages of controls. The combination of my team lead's review and my review is then sent up to the government contracting agency's authorizing official. The government contracting agency (GCA) is the customer for which DCSA serves as the cognizant security authority. All facility packages are sent up to the authorization official (AO) at the GCA, and they determine if they're okay with accepting any residual

risks found in the package. Once the AO is satisfied that the residual risk is addressed sufficiently, the AO approves the authorization. However, if the AO returns the package, they'll communicate the deficiencies to the team lead, and I will communicate these deficiencies to the facility for correction.

To paint a picture, a common example of how a facility is not compliant is the Control PE-19, which deals with TEMPEST mitigation. TEMPEST is the investigation and control of compromising emanations from telecommunications and automated information system equipment. The PE-19 is a contractual requirement that is outlined in the DD Form 254, a DoD contract security classification specification. Generally, TEMPEST is not required in the continental United States, and facilities interpret that to mean that the control is not applicable, writing in N/A. But the control itself is still applicable, so the facility has to state that they've reviewed the DD-254 and validated no TEMPEST requirements. So, in this case, they're non-compliant with PE-19, and won't be until they do the validation and correct the implementation and compliance status.

On average, about 60% of my time is onsite at a contractor facility and 40% in the office. I also spend a lot of time coordinating and supporting the industrial security representatives (ISRs) when they are doing their facility assessments. In addition to that, my team and I support the Defense Information Systems Agency's Command Cyber Readiness Inspection (CCRI) program. The program is designed to increase accountability and improve the overall security posture of the Department of Defense Information Network (DoDIN). Similar to what I already do, we look at cyber vulnerabilities in federal agencies, within and outside DoD, and provide information on how to improve their missions' operational risk. The CCRI program is an additional duty, and you have to volunteer for it.

Q: How do you cooperate across the field office?

A: I work in very close coordination with the ISRs and the information systems security professionals (ISSP) in my field office. When a facility is going through what is called an Enhanced Security Vulnerability Assessment (ESVA), DCSA sends an integrated team that consists of, at minimum, an ISR, a Counterintelligence Special Agent (CISA), and an ISSP (when there are classified systems involved). We coordinate closely regarding workload, input into the "methods of operation/ methods of contact" rating matrix, and writing a thorough report that outlines any vulnerabilities found, corrective actions taken, and open vulnerabilities.

Q: What is the most challenging aspect of your job?

A: The most challenging aspect is probably providing training to contractors so that they understand the control language and know what to put in their plan of action. For example, the PE-19 control will tell industry that they need to "protect the information system from information leakage due to electromagnetic signals emanations." However, I'll go in and give supplemental guidance that the control language doesn't convey, like the TEMPEST example we talked about earlier. Once they understand what they have to do, it becomes pretty clear.

Q: What's your favorite part about being an ISSP?

A: My favorite part is the CCRI program because I get to travel, and I get to see how other regions are approaching system reviews. The CCRI program in itself is very interesting because you feel like you really are at the tip of the spear. We're talking about a network that spans the globe since it's part of the Department of Defense Information Network (DoDIN). You feel like you're making a real impact in securing the information systems and minimizing the risk to the network, and in turn, to the warfighter.

Q: How does an ISSP support the CTP mission?

A: As an agency, we are tasked by the president and secretary of defense to ensure contractors are compliant and operating according to the NISP. By securing information systems and minimizing the risk to networks, we are assisting in delivering weapons systems that are uncompromised. That is an essential job for national security, if we (DCSA) are successful, then the contractor is successful, and the warfighter is protected, thereby making the country safer.

OVERSIGHT OF ACCESS-ELSEWHERE COMPANIES FOCUSES ON RISK IDENTIFICATION MITIGATION

By Andrew Parker
Critical Technology Protection

The National Access Elsewhere Security Oversight Center (NAESOC) administers DCSA's oversight mission for access-elsewhere companies, or companies that do not have a requirement to access classified information at their location. With nearly 3,500 facilities already assigned and preparing intake of additional companies, NAESOC enhances the National Industrial Security Program (NISP) by identifying and mitigating risk for these selected non-possessing facilities.

Traditionally, when a facility enters the NISP, it is assigned an industrial security representative (ISR) based on the physical location of the company. Within the NAESOC, facilities can be located across the country and don't have a single ISR, but rather a team. The NAESOC prioritizes risk identification and mitigation rather than the type of facility, technology, or geography. Oversight is conducted in a holistic manner during scheduled engagements.

NAESOC's call center is the main point of contact for customer service. Through email, secure National Industrial Security System (NISS) messaging, and call center support, it has fielded over 3,500 requests, providing oversight and guidance as well as individual responses to facility security officer (FSO) queries. In addition to industry support, government security and acquisition officers also receive guidance and training. NAESOC maintains a dedicated page on the DCSA website to keep its customers informed of key updates, explanations of self-help actions that companies and FSOs can implement to augment their own current security measures, and links to additional resources and training.

Outreach and education are a large part of NAESOC's mission. Already accustomed to providing virtual presentations to geographically dispersed industrial security awareness councils and other outreach efforts prior to COVID-19 restrictions, NAESOC has provided over 30 customer-facing engagements to explain its functions and benefits to approximately 3,800 attendees.

The three functions of NAESOC — identification, prioritization, and mitigation — are aligned along three teams: Strategy and Communications, Continuous Vetting – Facilities, and Active Monitoring and Engagement.

The Strategy and Communications Team identifies and tracks key metrics addressing facility security, which are then analyzed for trends and similarities. Then, once triaged, teams are assigned to apply mitigations to address any identified vulnerabilities. Approaching the risk rather than the facility provides NAESOC the capability to identify the most urgent and greatest opportunity to address mitigation within the population, providing both targeted and enterprise solutions. For example, this year, NAESOC identified a population without access to NISS. Team members contacted these facilities, explained the NISS access requirement, provided training, and ultimately approved more than 1,700 NISS accounts.

The Continuous Vetting – Facilities Team is a crucial participant in the risk identification process within NAESOC. Through oversight of facility reporting, the team assists industry in processing change conditions and security violations, in addition to mitigating vulnerabilities outside of security reviews. NAESOC's continuous vetting capability has been augmented with an analytic, open source, continuous monitoring solution that supports risk identification and prioritizes targeted facility engagements.

The Active Monitoring and Engagement Team is revolutionizing continuous monitoring engagements and security reviews in a virtual environment, using a blend of live telephone calls and NISS messenger emails. The team also incorporated the NISS facility profile update package as part of its virtual security review process, creating a collaborative approach and reinforcing industry's responsibility to control their own information. This real-time method ultimately takes the place of email-based engagement, providing more targeted, personal discussion, follow-on questions, and deeper analysis of the company's security program and business practices. These engagements conclude with immediate feedback, risk identification and resolution, and education as necessary.

The NAESOC is further organized along the Department of Defense's task force concept. Key partners within DCSA augment NAESOC's risk identification and mitigation mission:

Counterintelligence (CI): NAESOC has established inroads with counterintelligence special agents (CISA) in the field to develop lines of reporting and coordination, providing rapid response for CI issues. The NAESOC CI team ensures the right attention, both locally and strategically, is provided to its assigned facilities.

Center for Development of Security Excellence (CDSE): NAESOC's dedicated CDSE liaison helps define the messages and training needed for NAESOC customers. This liaison has been supportive in targeting NAESOC facilities for messaging, as well as developing fundamental communications such as webinars focused on facility knowledge requirements.

Vetting Risk Operations Center (VROC): A VROC support team puts NAESOC at the front of personnel clearance (PCL) issues that impact a facility's clearance (FCL).

Critical Technology Protection (CTP): The CTP enabler and detailees from the field have been vital assets in ensuring that NAESOC remains flexible in its response capability. The CTP enabler is a dedicated member of NAESOC, assigned from a field location to expand customer outreach. Detailees are volunteers provided by the field that develop and maintain NAESOC operations while it reaches full staffing. They have been instrumental in designing and validating NAESOC processes and providing oversight to the many facilities incorporated into NAESOC.

For more information on NAESOC, please visit www.dcsa.mil/mc/ctp/naesoc/.

A DAY IN THE LIFE: BACKGROUND INVESTIGATION

DCSA's background investigations are the first step in the personnel vetting process. These individuals help to deliver efficient and effective background investigations, adjudications, and continuous vetting to safeguard the integrity and trustworthiness of the federal and contractor workforce.

ANDREW BRAMSCH

Investigative Assistant, Background Investigations, Central Region

Q: What is a typical workday for an investigative assistant (IA)?

A: IAs conduct and report the results of investigative record searches, typically law enforcement and court records. They are also responsible for field office administrative support, including retention and destruction of personally identifiable information (PII), maintenance and replacement of government-owned vehicle, office supply ordering, maintaining annual compliance requirements, shared calendars, and more.

In other words, chaos. I tell people I'm either working 0% or 100%, and it's mostly 100%. You've got to be really flexible in this job. Each day, I go in and get the daily download of new cases, answer emails and phone calls about different subjects, like cases I worked, agents asking for help on travel, leave questions, and everything you can think of in terms of logistics.

Q: How many agents do you work with or assist?

A: It's different from day to day, but it's usually about 23 agents. In my office, there are two field offices, so sometimes I help the other side too, and that's an additional 21 agents. Requests can be anywhere from, "please fax this" to "please provide regulations and procedures." I help with a lot of IT questions, before agents call the help desk.

Q: On average, how many cases do you receive a day or a week?

A: That also fluctuates. The cases that I handle are the official personnel folders. I also do law checks for Illinois, Indiana, and parts of Kentucky. Sometimes, I also help Chicago with their police checks.

Q: What do you think is the most important aspect of your job as it relates to the DCSA mission?

A: Fact checking is the most important aspect of my job, making sure things are done right. If I find something that needs to be done, or is outside of my capabilities, I make sure to get it to an agent. I would say logistical things are important — things that the agents aren't aware of — like travel, vehicles, things like that. IAs are the glue that holds the logistics section of the mission together.

Q: What aspect of your job takes up the majority of your day?

A: While I stay busy with my own fieldwork assignments, a good portion of my day is spent providing whatever support the special agents and special agent-in-charge (SAC) of my offices need, which can vary greatly from day-to-day.

Q: What is a fact about your role that others might not know?

A: When you transfer a car from General Services Administration (GSA), there is all this paperwork to get the car to the agent. I'm developing video guides for agents on how to do this.

VIRTRE TIGGLE

Special Agent-in-Charge, Northern Region

Q: What is a typical day like for a special agent-in-charge (SAC)?

A: No two days are the same. I can always expect some sort of curve ball, whether it's a new project or an employee relations matter, but in general, my day starts very simply with checking emails. I take a look at the cases that have come in, and I assign and distribute work to my team members based on their current workload and experience. Once that is done, I spend time reviewing cases that have been completed and entered into the case processing system to ensure they are accurate, complete, and in compliance with our standards — a quality check before it goes to the Quality Team for a more thorough review.

I also like to take some time throughout the day to check in with my team members. I manage two teams with almost 30 people total, so I usually call or message two employees each day just to see how they're doing and to find out if there's anything they need help with. I also routinely check in with my supervisor to see if there are any special tasks or projects that need my attention.

> *Part of my job is to ensure they feel appreciated and validated so that they can be their best. We have an important mission, and I like to remind them of their importance in achieving it.*

Q: What do you think is the most important aspect of your job as it relates to the DCSA mission?

A: Hiring has been a big deal. I have to vet people and provide my opinion on whether or not I am confident they can do the job and respect the mission. I take that very seriously. The organization makes a significant investment in every investigator that we hire. It can take up to a year for an agent to become fully productive, and that's a lot of time to invest in a person.

I also take my responsibilities to our existing employees seriously. Part of my job is to ensure they feel appreciated and validated so that they can be their best. We have an important mission, and I like to remind them of their importance in achieving it.

Q: What aspect of your job takes up the majority of your day?

A: Emails, by far, take up the majority of my day. I get tons of emails throughout the day, and I try to stay on top of them and respond in a timely manner. I don't want any lack of response by me to result in a case being delayed.

Q: What is the most challenging aspect of your job?

A: I'd have to say that time management is the most challenging aspect of my job. There are a lot of moving parts when you're a SAC, and it can be tough at times to make sure everything gets done. I was also selected for the agency leadership development program, so I have to make time to work those projects as necessary.

Q: What is something about your role that others might not know?

A: Some people think that SACs just assign work, but it's important for everyone to know that we are also that middle voice. We get management's voice down to the employees, and we provide feedback upward to management so that employees' voices are heard and considered.

We also act as an advocate for the agents and work on projects to help them. For example, we worked with the Office of Naval Intelligence to accommodate office space for our agents. We conducted a bit of a hub there and began to develop a good working relationship, which enabled us to request and receive some dedicated space. We are continuously speaking to other facilities on the agent's behalf to accommodate requests such as this one.

LISA ALLEN

Investigative Assistant,
Personnel Investigations Center

Q: What is a typical day like as an investigative assistant?

A: A typical day for me is working on cases, processing passports, and checking emails. First, we have to determine which agency the case is coming from, research the case, and finally, request all necessary documents. Once all the research has been completed, then we can process the case. After all the documents have been researched, I may need to get some assistance from my supervisor or one of my coworkers if there is a case that is missing some required information.

Q: What is the first thing you do when you get a new investigation?

A: When we first get a case, we examine it to find out where the applicant is currently and where they have previously worked. I may look at every possible place I think an applicant has worked, but sometimes the case needs to be returned to the subject to specify the agency(s) that they have worked for, but that's rare.

Q: What do you think is the most important aspect of your job as it relates to the DCSA mission?

A: The most important aspect of my job is protecting national security. This means paying attention to every detail in an applicant's file to ensure that it is well researched, properly vetted, and the facts are correct.

Q: What aspect of your job takes up the majority of your day?

A: Research takes up majority of my day, as I need to ensure that each case has the proper facts and documentation, and that it's not missing any relevant information that is important to the case.

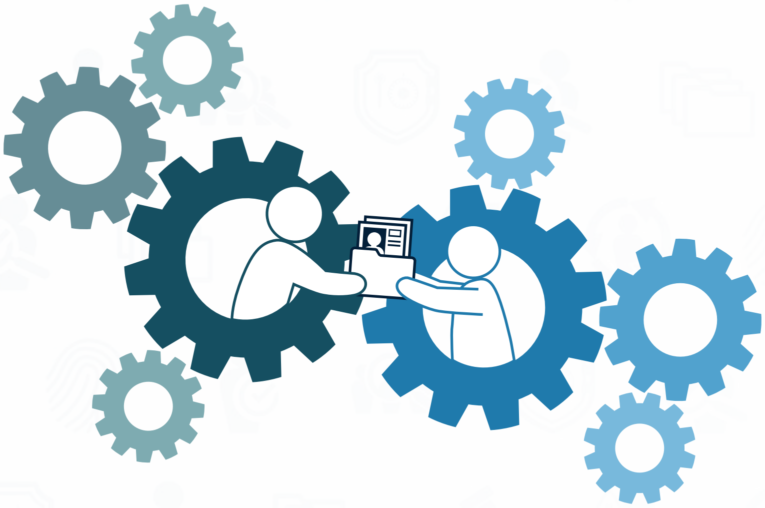
Q: What is the most challenging aspect of your job?

A: The most challenging part of my job is navigating the different information systems used for research as well as the research itself. Another challenge is the applicant might not provide enough information or maybe there's information that wasn't reported by them. Acronyms are another challenge. If you are not aware of the acronyms they use, then you have to look it up before you can move on with the research.

Q: What is a something about your role that others might not know?

A: The Quality Team deals with a lot of information, but we do not see it as just another case — we understand that it's actually a person who is waiting on his or her clearance. An applicant could be waiting to deploy or waiting to start a job to care for his/her family. This is also time that an agency or military branch is going without the support the applicant can provide. We see the importance of every case.

We take our jobs of ensuring adjudicators have a "whole" picture of each applicant very seriously. We want to do our part in helping the federal government employ the best, most trustworthy workforce that we can.



A DAY IN THE LIFE: ADJUDICATION

DCSA's certified adjudicators apply regulations, executive orders, and governmental directives to assess an individual's loyalty, trustworthiness, and reliability in determining whether it is in the best interest of national security to grant that individual eligibility to access national security information.

CORRINE EDMONDS

Adjudicator, Division 5, DoD CAF

Q: What kind of skills are required of an adjudicator?

A: Being an adjudicator requires the ability to multi-task, pay close attention to detail, stay alert and focused, and interact professionally with command members at all levels. Adjudicators need to possess exceptional organizational skills, as well as superb oral and written skills, all while being able to work with little supervision. Adjudicators should also possess excellent typing abilities and the skills to prepare documents with minimal errors before sending them for review. All of these attributes are required when making appropriate determinations on security clearance eligibilities in order to remain in accordance with all applicable policies and procedures.

Q: What is the first thing you do when you get a new case?

A: The first thing I do is check the position, type of investigation, and the agency that is requesting eligibility. This helps me decide what "route" I am going to take and determine if this is a case I am able to work or if I need to transfer it to another functional area. This also helps put me in the right frame of mind when reading the case and applying required Federal Investigative Standards (FIS). A case can take many different turns before a decision is made. I might need to order or request files that were not included with the case or for something that happened after the investigation closed, compose and send memorandums, request supplemental information, or provide a notification of intent to deny or revoke a subject's security clearance eligibility.

Q: What do you think is the most important aspect of your job as it relates to the DCSA mission?

A: I believe the most important aspect of my job is honesty and integrity. Being honest and impartial are key to being an effective adjudicator.

Q: What aspect of your job takes up the majority of your day?

A: The majority of my job is reading multiple and diverse investigations and assessing the information against the national security adjudicative guidelines.

Q: What is the most challenging aspect of your job?

A: Maintaining honesty and integrity is sometimes the most challenging aspect of my job because it is extremely important not to let your personal beliefs persuade you from making a sound decision.

Q: What is a something about your role that others might not know?

A: Being an adjudicator has made me an efficient speed reader.

DEVON MIDDLETON

Adjudicator, Division 2, DoD CAF

Q: What is a typical day like for an adjudicator?

A: An adjudicator spends a typical day reading about and analyzing the lives of individuals seeking clearance eligibility for a position in the military, civilian, or industry, and using this information to determine whether the individual is loyal, trustworthy, and reliable. We accomplished this by reviewing a completed national security investigation that contains a series of database results, listed questions, and responses from the individual and, if required, a personal interview. Once an adjudicator reviews this information, we analyze it using the 13 national security adjudicative guidelines laid out in the Security Executive Agent Directive-4 (SEAD-4) to apply a whole person concept and make an unbiased security determination. It is important to note that adjudicators don't "give" individuals a clearance, they only determine whether they are eligible for one. The agency sponsoring the clearance is the one who ultimately "gives" the clearance.

Q: What is the first thing you do when you get a new case?

A: The first thing I do when I get a new case is to mentally create a snapshot of the individual using general details about the case. These can be details such as being a new or current government employee, having current or previous eligibility, and whether the individual is military, civilian, or industry. I review a page contained in the completed investigation that provides queried database results, and I take note of concerns to be aware of, such as law enforcement records or financial issues, before reviewing the security questionnaire. These first steps help the adjudicator turn the data into a person, which is vital when trying to create the whole person concept.

Q: What do you think is the most important aspect of your job as it relates to the DCSA mission?

A: The most important aspect is an understanding that as an adjudicator, you are the final gatekeeper in a lengthy and complex vetting process that many individuals have worked hard on before it got to you. Your decision about the loyalty, trustworthiness, and reliability of the individual is the culmination of these efforts — it directly affects national security and should not be taken lightly.

Q: What aspect of your job takes up the majority of your day?

A: The majority of my day is reading and analyzing. I read a little, I think a little, and then I read and think some more. As I go through the investigation, I like to think of my eyes as searchlights. At first, the beams of light are wide, taking a wide sweep of the individual. The beams begin to narrow as I encounter adverse information and look closer at the individual and analyze the information for patterns. Because people are complex, the information you encounter can be as well, and this may require additional resources, such as a multitude of government databases or internal sources to help assist in your analysis.

Q: How do you prepare for an interview?

A: Interviews, by their very nature, are a stressful experience for any person. I prepare for an interview by trying to relieve stress and do something enjoyable such as exercising. I also try to build confidence by prepping with possible questions or doing research about a topic. Finally, it's important to remember to just be yourself and to give it your best effort.

Q: What is the most challenging aspect of your job?

A: The most challenging aspect is to remind myself about the human element of adjudications while analyzing information. People are not machines — they are not perfect. They come from a variety of backgrounds and have different life experiences. In fact, it is these different life experiences and backgrounds that make them so valuable to the government workforce. There is a tendency as an adjudicator, since you read about so many people, to forget how important this position is to the individual. Though the interests of national security are always at the forefront of your mind, it is important to treat each case as important as this position is to the individual.

Q: What is something about your role that others might not know?

A: After reviewing thousands of investigations on individuals, I can state that the majority of people are good, honest, and want to come together for the common goal of protecting our national security. I am proud to be a part of the government workforce and enjoy my role as an adjudicator. There are new challenges every day and no two cases are the same. I am excited about the future of this newly created agency and look forward to seeing how the adjudicative process evolves.

A DAY IN THE LIFE: COUNTERINTELLIGENCE

DCSA's Counterintelligence mission is the federal government's strongest link between the nation's industrial base, the U.S. Counterintelligence and Intelligence Community, and federal law enforcement. The following team members help with effective communication and information sharing to identify threats to cleared U.S. personnel and our nation's critical technologies.

ABIGAIL "ABBY" MADDEN

Counterintelligence Special Agent, Northern Region

Q: What is a typical day like for you?

A: On a typical day at work, I check my emails and dive into my work. Work could be anything from writing reports, triaging raw reporting from industry, and working with cleared contractors to answer questions or provide feedback. It could mean planning for an upcoming Enhanced Security Vulnerability Assessment (eSVA) or even putting together the Dart Board, which is a monthly collection of open source articles that are sent to the Red Dart counterintelligence (CI) groups around the country. The Red Dart is a national CI group that has chapters in many major U.S. cities. It allows for discussion and CI collaboration among member agencies, such as FBI, DCSA, or even the U.S. Coast Guard, to name a few.

> *"I'm very much an extrovert, and I love giving briefings and being put on the spot or hearing thought-provoking questions from the audience.*

Some of my favorite days are when I can go to a cleared contractor's location to provide a briefing. I'm very much an extrovert, and I love giving briefings and being put on the spot or hearing thought-provoking questions from the audience.

Another aspect of my work that I find very interesting is processing raw reports from industry. One day, I may get a report of a complex monetary scam, and the next day I could get a report about a potential insider threat. I find it most gratifying when I can provide my cleared contractors with feedback about their reports and recommend best practices to avoid the situation in the future, or how to recover from it. I particularly love it when I can take disparate reports from my area of operations, or even other government agencies, and begin to see a pattern of activity. I consider myself a creative person, so I think this aspect of my job enables me to use my creativity by looking at problems through different lenses, researching issues, and learning about all the new and old ways our adversaries work.

Q: What do you think is the most important aspect of your job as it relates to the DCSA mission?

A: I think the most important aspect of my job is supporting and partnering with industry. Every DCSA office has a large area of operations, whether in miles driven or number of cleared contractors we support. No one, not even counterintelligence special agents (CISAs), can be everywhere at once or support everyone. That's why it's so incredibly important to communicate with our industry partners so they can do their best to posture their security programs appropriately.

Q: What aspect of your job takes up the majority of your day?

A: Report writing and updating trackers takes up the majority of my day. I take pride in how I'm able to convey complex topics and issues in an understandable manner. I always try to keep in mind that another CISA could use my report 10 years in the future, and I cannot assume that they will know about all the threats or current events affecting my reporting today.

Q: What is the most challenging aspect of your job?

A: The most challenging aspect of my job is also one of my favorites. In the field, we can often be separated by distance from our region or headquarters, which often times means that getting support and resources can be difficult. This can be challenging because I don't always have the tools I need to properly do my job. However, this also allows me to be creative with how I approach a lack of resources. For example, last year one of our larger contractors hosted a security fair for their employees. At the time, we had yet to receive anything with the new DCSA seal on it, and I needed to figure out something the employees could take with them that would also reinforce the CI and security messages. I came up with the idea of going to the Center for Development of Security Excellence (CDSE) website and printing security posters, at about the size of a postcard, so employees could hang them in their cubicles. Everyone really liked them, and the event was a success!

Q: What is something about your role that others might not know?

A: Some may know this, but I think it's important to point out that even though we have a fancy and exciting sounding title, your average intelligence professional will work a notable or exciting case/ investigation probably three times in their entire career. Anything above that is unique, in my opinion. Some look at this statistic as a good thing, meaning CI threats don't happen too often. While others see it that CI threats happen all too often, but we are unable to track down enough information about them to really work a cohesive case or investigation.

Both sides of the argument have their points, and it's difficult to know who is right. The main message still remains: Sometimes our jobs are not as exciting as they sound, but they are still important. It's also implied that an intelligence professional may have a huge impact within their career but may never find out about it because the threat never came to fruition. CISAs have become accustomed to celebrating our small wins and successes, and that keeps many of us driving forward.

HECTOR C. RODRIGUEZ

Region Collection Management Officer, Capital Region

Q: What is a typical day like for you?

A: As a region collection management officer, I'm responsible for the collection process of counterintelligence (CI) information and guiding counterintelligence special agents (CISA) to focus their efforts on intelligence collection requirements and DCSA priorities. Intelligence collection requirements drive all intelligence, and the purpose is to process information and turn it into relevant, actionable intelligence. One aspect of this job is there is something new just about every day, and I have to remain flexible to adjust to any new priorities that may surface during the day.

My typical day starts with reviewing emails and my calendar to determine what meetings I have scheduled for the day. Juggling multiple tasks at once is a daily occurrence, while I take care of any time-sensitive tasks or projects, such as personnel issues that may need my attention. I also conduct reviews and approve reports written by CI special agents, including any products produced by our analysts.

Most of us are teleworking now due to COVID-19 restrictions, and that brings additional challenges with how we conduct our mission. All of us have had to adjust to how we conduct our work on unclassified systems. Relying on various virtual tools to conduct CI activities is not ideal, but we have adjusted in order to make sure the mission is not impacted.

Q: What do you think is the most important aspect of your job as it relates to the DCSA mission?

A: The people are always the most important aspect since, without them, the mission does not get accomplished. The ability to work together with other DCSA directorates, Intelligence Community (IC), law enforcement agencies, and cleared contractors is another important aspect of this job. In working with others, we have to be able to increase awareness and understanding of the threat. The key to any effective CI program is educating people to help them recognize the types of suspicious activities and behaviors that should be reported and identify how to report them. Receiving, analyzing, and disseminating reports of suspicious contacts or activities submitted by cleared contractors, and assisting them in applying appropriate countermeasures, is also an important part of what we do. It truly takes a collaborative approach to be able to protect national security, and everyone, regardless of their position, has a role in this effort.

Q: What aspect of your job takes up the majority of your day?

A: Being in a supervisory position has no shortage of work, and while it has its challenges at times, it's also a rewarding position. I have administrative duties, which tend to keep me busy during certain days, and I am responsible for providing quality control and oversight on intelligence reports written by CI special agents. I am also part of multiple internal working groups for various DCSA initiatives. We are also experiencing an increase in new hires coming onboard, and I will be responsible for training the new CI agents on DCSA's CI processes and procedures. Overall, there is no set answer for what takes up the majority of my day, since the answer will vary depending on what day it is, which makes this position appealing.

Q: What is the most challenging aspect of your job?

A: Cleared contractors are under a persistent threat from our adversaries, so one of the most challenging aspects of this job is the ability to detect these attempts and be ahead of the threat. Adversaries use multiple and varying avenues of attack against cleared industry. Unfortunately, we find ourselves in situations at times where we come across information which indicates a technology has been compromised. When foreign adversaries are successful, it damages national security, reduces the U.S. technological advantage, and increases the risk to the warfighter. Ideally, we want to be in a position in which we can anticipate what the adversary wants and know how they will try to obtain it so we can work with our industry partners to mitigate their collection efforts.

Q: What is something about your role that others might not know?

A: DCSA CI does not have the authority to conduct investigations, but we work as a force multiplier for those agencies that do. Our access to cleared industry provides significant operational and investigative advantages to the IC and law enforcement agencies we support. We want to be able to put actionable information into the hands of the agencies who can act on it. Everything we do is in an overt capacity, which means we do not hide in the shadows while doing our job.

DCSA RECOGNIZED WITH COUNTERINTELLIGENCE AWARDS

DCSA received recognition in four categories of the 2020 Intelligence Community National Counterintelligence (CI) and Security Professional Awards sponsored by the National Counterintelligence and Security Center (NCSC). The award program recognizes CI and security practitioners for exceptional performance in 19 categories.

The CI Cyber Division received the Countering Technical and Cyber Threats Team Award. The team implemented analytic processes through deployment of the Joint Cyber Intelligence Tool Suite (JCITS) to proactively detect foreign cyber threats to cleared contractor networks, mitigating previously undetected malicious activity.

DCSA Director William K. Lietzau (left) presents Richard Naylor, chief of the Counterintelligence Cyber Division, with the Countering Technical and Cyber Threats Team Award. (Photo by Christopher P. Gillis, OCCA)

Nick Luce, CI special agent in the Phoenix Field Office, received the Individual Award for Industrial Security. Luce advanced national security by creating more than 4,000 suspicious activity reports and 330 intelligence information reports, which generated 23 investigations (or operations), access removal of 30 entities, and five arrests.

“I am greatly honored to receive this award,” said Luce. “I’d like to recognize the professional colleagues I have the pleasure to work with, day in and day out, in the Phoenix Field Office. I’d also like to recognize the industry partners I am fortunate to work with — highly dynamic facility security officers (FSO) and key management officers that place significant value on delivering uncompromised technology to our warfighters, along with other organizations around the country, and information technology professionals, that are committed to securing critical information wherever it resides.”

The San Diego CI and Security Team received the Team Award for Industrial Security. The team’s innovative collection strategies and security approaches resulted in over 3,000 suspicious incident reports, 200 intelligence information reports, and over 500 referrals leading to investigations that disrupted 30 threat actors.

The Expedited Screening Center (ESC) received the Insider Threat Detection Team Award. In response to an urgent Secretary of Defense policy, the ESC established a robust international military student vetting program to proactively identify risks and maintain trusted international strategic partnerships.

EXPEDITED SCREENING CENTER EXPANDS MISSION TO STRENGTHEN STUDENT VETTING

In 2019, under the direction and guidance of the Secretary of Defense (SECDEF), DCSA established the Expedited Screening Center (ESC) to improve vetting of personnel with potential foreign influence, foreign preference, or allegiance concerns. The ESC screening approach optimizes intelligence data sources and human analytics to detect potential risks in these areas. The ESC began screening military accessions and a limited number of other Department of Defense (DoD) personnel, providing faster and more efficient vetting for individuals with those potential concerns.

> ***"In a short amount of time, we were able to demonstrate the value of an expedited screening capability for identifying certain forms of risk within the workforce."***
>
> **Joshua D. Martineau, chief of the ESC**

In December 2019, an international military student (IMS) attending training at Naval Air Station Pensacola executed a terrorist attack that killed three service members and injured eight individuals. In the days immediately following the attack, the SECDEF directed the ESC to screen all international military students currently training in the United States. The initial screening proved invaluable, as it identified students with undisclosed connections to foreign intelligence entities and connections to organizations that posed a potential risk to U.S. critical technology.

"Less than a week after the tragic terrorist attack in Pensacola, we were given a short deadline to screen many of those IMS already in the U.S., in order to help identify other immediate potential threats that could result in a loss of life," said Martineau.

There were multiple challenges to incorporating the IMS screening mission, including finding a way to rapidly screen hundreds of individuals using existing resources. However, the ESC workforce surged through late nights and weekends to complete the initial screening requirement ahead of schedule.

The ESC is now expanding to screen approximately 22,000 international military students who train annually in the U.S. and will do so prior to the Department of State's visa issuance. These efforts will seek to more closely align IMS screening, vetting standards, and procedures with those applied to U.S. personnel.

> ***"Our partnerships with our allies are crucial to our defense strategy, so we were asked to take immediate steps to strengthen vetting for international military students for DoD."***
>
> **Heather Green, director of the Vetting Risk Operations Center (VROC)**

VROC immediately enhanced the ESC's capability to vet this additional population, implementing new direction from the Under Secretary of Defense for Intelligence and Security (USD(I&S)). Moving forward, USD(I&S) and DCSA will focus on developing a continuous review capability for international military students in the U.S. They'll also work to facilitate information sharing between ESC and the Department of State, ensuring relevant information is available during the visa process.

A DAY IN THE LIFE:
NATIONAL SECURITY LEARNING CENTER

These DCSA personnel provide the Department of Defense (DoD) with a security center of excellence, professionalize the security community, and provide security education, training, and certification for DoD and industry.

ADRIENE BROWN

Marketing and Communications Team Leader and Events Program Manager, Center for Development of Security Excellence

Q: What is a typical day like for you?

A: Every day is a new adventure. I'm managing multiple projects from both a marketing and events perspective. There's always something new and unexpected things that come up. I love working at home. I'm impressed that I'm more productive and appreciate not dealing with the stress.

Q: What is the first thing you do when you get a marketing/event objective?

A: The first thing we do with an event is work with the stakeholder to find out what they are trying to achieve, what audience they are trying to reach, what message they want to convey, and what actions we need to complete.

Q: What do you think is the most important aspect of your job as it relates to the DCSA mission?

A: The most important aspect of our job is to ensure that the Department of Defense (DoD) enterprise is aware of the training resources available through multiple outlets, such as the Center for Development of Security Excellence (CDSE) Pulse newsletter and weekly flashpoint message.

Q: What aspect of your job takes up the majority of your day?

A: Meetings, meetings, and more meetings take up the majority of my day. They can be both effective and counterproductive.

Q: How do you prepare to be a marketing/event professional?

A: I have been doing event planning the majority of my adult life, and marketing tactics are an essential aspect to ensure the event is successful. Some of my volunteer work has required a marketing plan, so it was a natural progression. When I joined CDSE, I started as the executive assistant for the director, then transferred to the training division, and worked at a couple of other sections in CDSE. I've learned the CDSE mission, but it wasn't a traditional way to get into event planning.

Q: What is the most challenging aspect of your job?

A: The most challenging aspect of my job is managing resources against the new requirements and expectations for the mission.

Q: What is something about your role that others might not know?

A: People might not realize how visionary you need to be in this role, but also detail oriented.

MATT BANDI

Quality Review Instructor,
National Training Center

Q: What is a typical day like for you?

A: My typical day depends on whether we are conducting a training class that day. When we have a class, the focus is completely on making sure each student has everything they need to be able to do their job. There is a bit of time during classes for small projects and the occasional meeting while other instructors are teaching, but all that gets pushed aside if a student has questions or needs some additional time on a particular topic.

On days when we do not have a training class, we spend most of our time working on our training materials. There is a substantial amount of material required for any training class including lesson plans, PowerPoint presentations, job aids, exercises, etc. All those materials need to be accurate, clear, and up to date at all times, which requires pretty constant attention.

> “
> *Guidance that seems simple and straightforward for an experienced employee can sometimes be unclear to someone just starting the job. It is our responsibility to figure out how to present that information in the clearest possible manner.*

Q: What is the first thing you do when you get a new training objective?

A: As part of our program's accreditation process, we follow the ADDIE Model — Analysis, Design, Develop, Implement, and Evaluation — for developing training. The overall objectives for a particular training are determined during the analysis phase. Next, we design and develop the training, after which it can be formally implemented. Finally, we review the effectiveness of the training during the evaluation phase.

Q: What do you think is the most important aspect of your job as it relates to the DCSA mission?

A: The most important aspect of my job is ensuring any student we deal with has everything they need to do their job and to do it well. Since we are typically train recently hired employees, this requires looking at all meaningful pieces of agency guidance from the perspective of someone who is brand new to the background investigation process. Guidance that seems simple and straightforward for an experienced employee can sometimes be unclear to someone just starting the job. It is our responsibility to figure out how to present that information in the clearest possible manner.

Q: What aspect of your job takes up the majority of your day?

A: I spent the majority of my day keeping materials updated and accurate. Even small changes in guidance or procedures can mean significant revisions to training materials. Beyond that, we are always looking for ways to improve our classes, and most new ideas require creating new materials or modifying existing materials.

Q: What is the most challenging aspect of your job?

A: For me personally, the most challenging aspect of my job is speaking in front of people. Like many individuals, it is not something I am naturally comfortable doing. I combat that apprehension by preparing as much as possible before conducting any type of training. I want to go into a presentation or discussion knowing exactly what I am going to say and how I am going to say it. I also spend plenty of time anticipating what types of questions I am likely to encounter beforehand.

Currently, while we are in a maximum telework situation, we are also facing the challenge of conducting meaningful training without the benefit of in-person contact. We have mostly utilized a blended approach, mixing video conferencing on Microsoft Teams with self-paced training via our Learning Management System. The early results of this method appear to be successful, as student feedback has been mostly positive.

Q: What is something about your role that others might not know?

A: Others might not know that we do not teach anything unless there is some sort of official written guidance to back it up. We can give our opinion or provide examples of best practices when specific guidance does not exist, but we are sure to clearly state when this is the case.

CDSE LAUNCHES OPSEC CAMPAIGN COURSE ON TWO PLATFORMS

SEES 4.2 MILLION COMPLETIONS

By Adriene Brown
Center for Development of Security Excellence

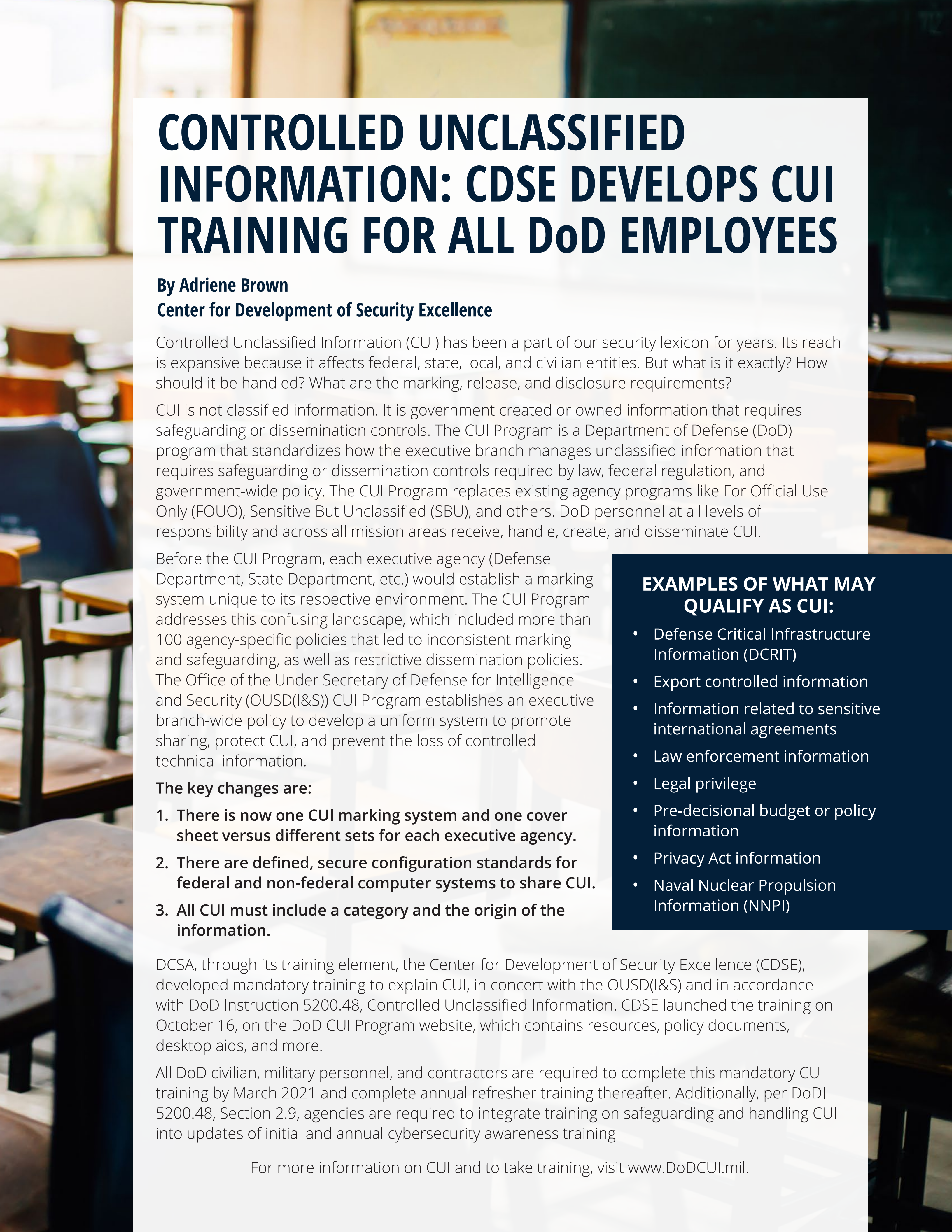
In June 2020, the Secretary of Defense's Operations Security (OPSEC) campaign kicked off with four mandatory courses and an introductory video, promoting best practices and addressing critical information leaks. Building upon successful execution as the federal provider for National Insider Threat Task Force (NITTF) awareness training, the Center for Development of Security Excellence (CDSE) was tasked with providing the OPSEC training courses as well as hosting the platform to deliver content.

The OPSEC campaign provided many challenges and opportunities for CDSE. First, CDSE needed to determine how to support the vast target audience for the campaign, estimated to be in the millions. After assessing its infrastructure, CDSE quickly determined that it would need both its platforms — the STEPP learning management system and the Security Awareness Hub — to support the OPSEC target audience.

In the first 30 days, more than 1.2 million users completed training from the OPSEC eLearning catalog — more than CDSE's total course completions for all of FY19. The vast number of users, coupled with a short deadline for the four trainings, ultimately still overwhelmed the two systems. Nevertheless, CDSE's mantra, "*not if, but how?*" kicked in, and the team worked diligently to improve system performance and balance the overload. Additionally, when outdated content was discovered in one of the courses, the CDSE staff worked tirelessly to overhaul the course and revamp the material within days.

Ultimately, the campaign's end date was extended by a month, from September 22 to October 22. By the end of the campaign, there were more than 4.2 million completions.

The OPSEC campaign truly tested CDSE's training systems capacity and provided many lessons learned. As a result, CDSE began testing a new capability that will monitor for peak system usage and automatically provide additional resources, when needed. While this capability is new to the environment, so is the need for CDSE's courses to reach millions of users. If successful, the new feature could help CDSE prepare for future high volume course access requirements.



CONTROLLED UNCLASSIFIED INFORMATION: CDSE DEVELOPS CUI TRAINING FOR ALL DoD EMPLOYEES

By Adriene Brown
Center for Development of Security Excellence

Controlled Unclassified Information (CUI) has been a part of our security lexicon for years. Its reach is expansive because it affects federal, state, local, and civilian entities. But what is it exactly? How should it be handled? What are the marking, release, and disclosure requirements?

CUI is not classified information. It is government created or owned information that requires safeguarding or dissemination controls. The CUI Program is a Department of Defense (DoD) program that standardizes how the executive branch manages unclassified information that requires safeguarding or dissemination controls required by law, federal regulation, and government-wide policy. The CUI Program replaces existing agency programs like For Official Use Only (FOUO), Sensitive But Unclassified (SBU), and others. DoD personnel at all levels of responsibility and across all mission areas receive, handle, create, and disseminate CUI.

Before the CUI Program, each executive agency (Defense Department, State Department, etc.) would establish a marking system unique to its respective environment. The CUI Program addresses this confusing landscape, which included more than 100 agency-specific policies that led to inconsistent marking and safeguarding, as well as restrictive dissemination policies. The Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) CUI Program establishes an executive branch-wide policy to develop a uniform system to promote sharing, protect CUI, and prevent the loss of controlled technical information.

The key changes are:

1. **There is now one CUI marking system and one cover sheet versus different sets for each executive agency.**
2. **There are defined, secure configuration standards for federal and non-federal computer systems to share CUI.**
3. **All CUI must include a category and the origin of the information.**

EXAMPLES OF WHAT MAY QUALIFY AS CUI:

- Defense Critical Infrastructure Information (DCRIT)
- Export controlled information
- Information related to sensitive international agreements
- Law enforcement information
- Legal privilege
- Pre-decisional budget or policy information
- Privacy Act information
- Naval Nuclear Propulsion Information (NNPI)

DCSA, through its training element, the Center for Development of Security Excellence (CDSE), developed mandatory training to explain CUI, in concert with the OUSD(I&S) and in accordance with DoD Instruction 5200.48, Controlled Unclassified Information. CDSE launched the training on October 16, on the DoD CUI Program website, which contains resources, policy documents, desktop aids, and more.

All DoD civilian, military personnel, and contractors are required to complete this mandatory CUI training by March 2021 and complete annual refresher training thereafter. Additionally, per DoDI 5200.48, Section 2.9, agencies are required to integrate training on safeguarding and handling CUI into updates of initial and annual cybersecurity awareness training

For more information on CUI and to take training, visit www.DoDCUI.mil.

COMMITTEE FOCUSES ON PROACTIVELY PROVIDING SECURITY TRAINING PRODUCTS

By Adriene Brown and Jason Steinour
Center for Development of Security Excellence

In August 2020, the Center for Development of Security Excellence (CDSE), in partnership with the National Industrial Security Program Policy Advisory Committee (NISPPAC), established the Government and Industry Security Training (GIST) Committee to enhance the availability of security training products and foster a proactive, risk-focused culture.

The GIST Committee, which will meet quarterly, is 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.

Partnership is central to its success, therefore, the GIST Committee is comprised of more than 30 industry and government partners who represent cleared industry, DCSA, and the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)). Industry members were selected to ensure balance and diversity of representation and experience. They include representatives from small, medium, and large facilities, including possessing and non-possessing facilities, and access-elsewhere facilities.

The GIST Committee differs from other stakeholder working groups, such as the DoD Security Training Council (DSTC), because its primary focus is to improve CDSE's training products, with an emphasis on industrial security training performance support tools.

The GIST Committee will play an instrumental role in the Government Employees with Security Responsibilities (GESR) Project (pronounced "jesser"), establishing a subcommittee that identifies focus group members and provides subject matter expertise for identifying training gaps. A recent training that needed analysis (conducted on behalf of the CDSE) revealed a desire for more training about security responsibilities that government employees are tasked with. It also very clearly revealed that these individuals are not always security specialists.

As a result, CDSE decided to take a more critical look at GESRs involving government security responsibilities. The GIST Committee and the GESR Project will investigate which roles in the various branches of service and government agencies fulfill security responsibilities, how to effectively reach audiences with training, and most importantly, what training is both required and requested by these varied audience groups.

NATIONAL TRAINING CENTER COURSE RECEIVES REACCREDITATION

By Rhonda Meehan
National Training Center

On November 5, 2020, the Federal Law Enforcement Training Accreditation (FLETA) board unanimously granted reaccreditation to the DCSA National Training Center's Investigations Case Analyst Program (ICAP). The ICAP provides background investigations training to DCSA quality reviewers and is taught at both the National Training Center (NTC) in Slippery Rock, Pennsylvania, and the Personnel Investigations Center (PIC) in Ft. Meade, Maryland.

> ***"The ICAP reaccreditation is the culmination of years of dedicated hard work within NTC and the strong bond we share with our FLETA partners."***
>
> **Colleen Coleman, NTC acting director**

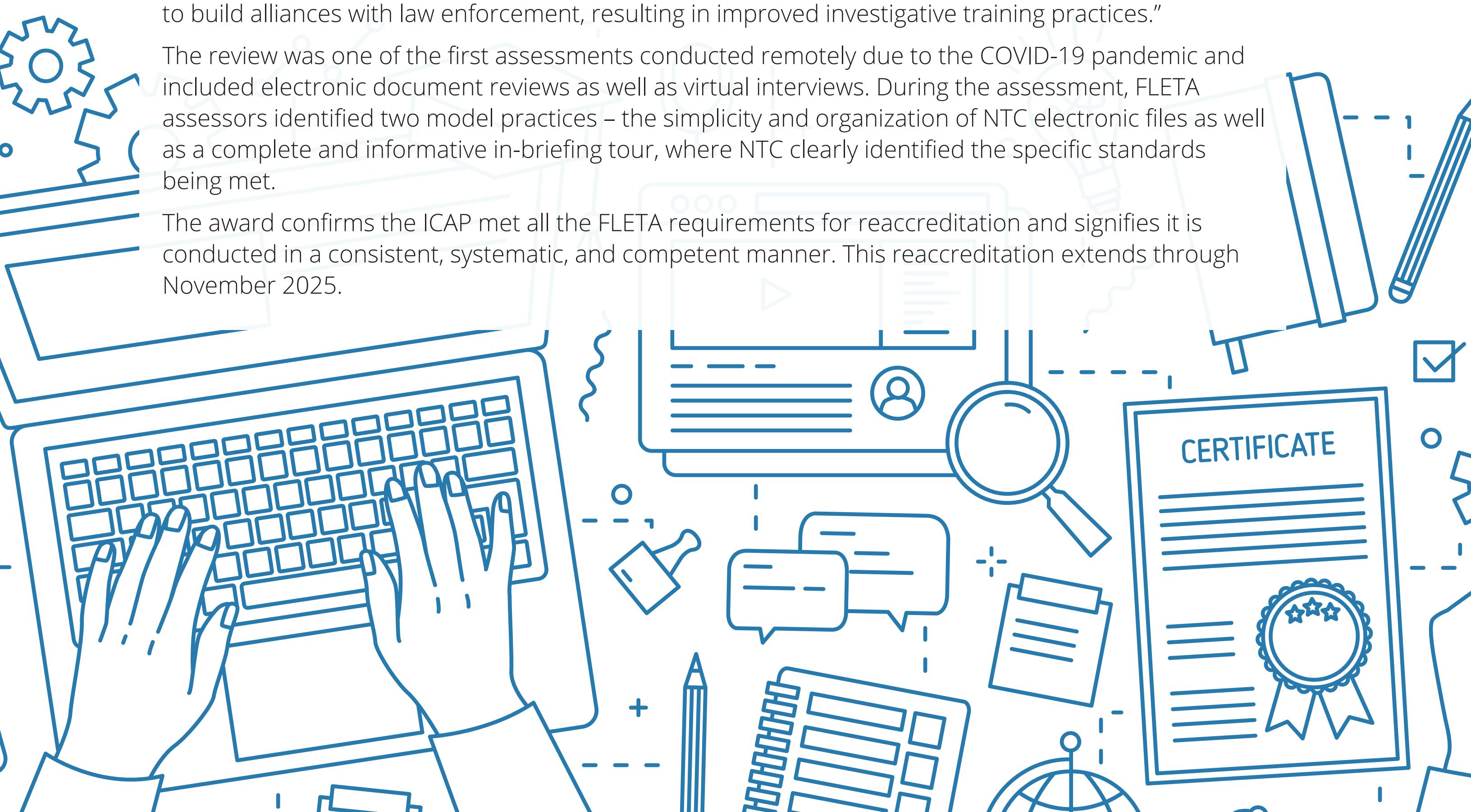
This is the first reaccreditation for ICAP, which received its original accreditation in November 2015 after nearly an 18-month process. Reaccreditation occurs every five years.

To achieve reaccreditation, NTC submitted ICAP to an independent review by a team of qualified FLETA assessors in July. The assessors reviewed all directives, policies, and evidence in the areas of program administration, staff qualifications and development, curriculum development, and training delivery. The review board examined ICAP's compliance with FLETA program standards, which were developed by training professionals and experts from the academic community to promote excellence in operations.

"The FLETA standards align with NTC's mission and vision for training geared toward protecting national security and the public trust," said Coleman. "In addition, FLETA accreditation allows the NTC to build alliances with law enforcement, resulting in improved investigative training practices."

The review was one of the first assessments conducted remotely due to the COVID-19 pandemic and included electronic document reviews as well as virtual interviews. During the assessment, FLETA assessors identified two model practices – the simplicity and organization of NTC electronic files as well as a complete and informative in-briefing tour, where NTC clearly identified the specific standards being met.

The award confirms the ICAP met all the FLETA requirements for reaccreditation and signifies it is conducted in a consistent, systematic, and competent manner. This reaccreditation extends through November 2025.



SUCCESSFULLY NAVIGATING LONG-DISTANCE RELATIONSHIPS

By Jennifer Norden
Irving Field Office, Texas

Human beings need direct interaction to establish and sustain almost any type of relationship, which is why long-distance relationships often bear a connotation of doom and inevitable failure.

At DCSA, the relationships we build make or break the success of our mission to protect national security information. Effective partnerships are not a distant goal for the DCSA workforce; rather, they are the expectation. But how do we achieve this when the security programs we support are geographically remote, especially in the time of COVID?

The Irving Field Office's geographic area of responsibility (AOR) includes North Texas — no small chunk of real estate by itself — as well as Oklahoma, Arkansas, and western Kansas. Nearly half of our facilities require more than a three-hour drive, while others require more than five hours, and a few involve a flight and a long drive. This is not unique to the Irving AOR. Many DCSA field offices manage territories that present significant challenges for providing live, on-demand support.

Long-distance relationships are notoriously tough in any context, but the expression "failure is not an option" couldn't be more appropriate in describing DCSA's determination to make them work. As the threats to our technologies continue to increase in intensity, complexity, and scale, it is ever more imperative that our DCSA team successfully works with all of our facilities, near and far, to collaboratively establish and maintain effective security programs. I asked my Irving team to share their long-distance playbooks to help highlight how they achieve success and get through the rough patches.

How do you approach starting a relationship with a facility that's in a remote location?

- That first conversation with a facility is make or break. "If our first impression doesn't convey sincere commitment to the facility's security program, the government stakeholder, and the warfighter, we undermine the prospects of a successful long-term relationship."
- **Senior Industrial Security Representative (SISR) Jeffrey Lee** says he "begins with presenting authenticity and an agreement of shared goals" and "developing mutual respect."
- "I send an email to introduce myself and schedule a phone call," another team member reported. "I start by creating a shared vision and mission."
- **Information Systems Security Professional (ISSP) Keith Williams** lays the groundwork for that commitment through demonstrating approachability and a supportive attitude during this first engagement. In other words, he says we have to be convincing when we say, "we're the government, and we're here to help." Especially when "here" means 200 miles away and when "help" is presumed to mean "find something the company is doing wrong."

What are some of the keys to success in maintaining partnership and transparency for remote companies?

- In long-distance relationships, and in the national security arena in general, everything ultimately boils down to establishing trust. There can't be commitment without trust. "Once an FSO, or facility security officer, knows he/she can trust me with

information, it is up to me to live up to that trust every day. In a distance relationship, this is vital," said **Counterintelligence Special Agent (CISA) Steve Michaud**.

- Availability and responsiveness are means of engendering trust, according to several team members. **ISSP Williams** strives to keep his email box emptied. "I do my best to answer all emails as quickly as possible, and at least reply that I am working on it if I am not able to fully research and provide an answer," he said. **SISR Amy Teets** agreed, "One of my key efforts is being available to the facilities and being responsive on emails."
- From first contact through many years of partnership, infrequent on-site time must be countered with more prolific communications, and sometimes alternative, engagement strategies. **Industrial Security Representative (ISR) Carlos Chandler** conducted a webinar with his remotely located FSOs to walk through how to submit condition changes to packages to DCSA. Chandler not only provided valuable information, but also used the event to encourage this remote FSO community to network and share their expertise.
- SISR Jeff Lee incorporates a "DCSA Day with Jeff" during his visits to Tulsa, so that he can interact with as many of the facilities as possible while in the area. **SISRs Chris Flitcraft, Amy Teets, and Darren Dennard** do the same in Lawton and Oklahoma City, Oklahoma; Wichita, Kansas; and Camden, Arkansas.
- The counterintelligence team doesn't stay under the radar, either. They send daily emails with threat information and counterintelligence resources so that FSOs can strengthen their countermeasures and increase threat awareness across the business enterprise.

How do you measure success for your oversight and support of long-distance companies?

- If DCSA employees effectively convey commitment and trust, then facility programs will start to mirror these tenets. "Facilities consistently mitigate their own administrative [vulnerabilities] using the Joint Personnel Adjudication System (JPAS), which involves regular maintenance, self-inspection, information sharing and documentation, contracting issues, account needs, etc.," explained **SISR Lee**. "The various FSOs and security staffs contact me regularly with updates and information."
- **ISSP Williams** offered examples of several industry information systems security managers (ISSMs) taking his recommendations to invest time in creating common control provider packages within the Enterprise Mission Assurance Support Service (eMASS), which, once approved, will expedite future plan creation by the ISSM, and shorten review times by DCSA.
- Likewise, ISRs and ISSPs noted that if they've done their job — sharing advice and expertise and providing a strong foundation of support for long-distance programs — FSOs are more likely to have the confidence to assume delegated roles allowed by policy and DCSA. These roles include approving their own closed areas, serving as designated government representatives for classified international shipments, or undertaking authorization responsibilities for classified information systems.
- For counterintelligence, success comes in the form of FSOs applying the threat products to their programs, raising the threat awareness level at their facilities, and reporting suspicious contacts and activities.

Can long-distance relationships work? Yes, with commitment and resolve, trust and communication, and empowerment and reciprocity. From my chief seat, if we've done our job establishing commitment and trust, the tough times will prove and strengthen the relationship, as both the company and DCSA will collaborate to find a solution. No one fights harder for their facilities than our first-line team of ISRs, ISSPs, and CISAs.

VIRTUAL BOOK CLUB EXPLORES LEADERSHIP CONCEPTS & BEST PRACTICES

By Quinetta Budd
Office of Communications and Congressional Affairs

"Today a reader, tomorrow a leader." — Margaret Fuller

When COVID-19 swept the country, employees soon found themselves working from home, and agency leaders sought ways to engage employees beyond work. The Employee and Leader Development (ELD) team, led by Dr. Bolton, chief of the Human Capital Management Office (HCMO), with support from Larry Cunningham, HCMO leadership development administrator and Ray Campbell, director of the Office of Diversity and Equal Opportunity (DEO), decided to offer a virtual book club to explore leadership development concepts with a geographically dispersed workforce.

In developing the Leadership Development Program (LDP), Cunningham initially reviewed more than 23 elements of successful leadership development programs and found that reading was among the top 10 elements. "Reading lets a person learn from others — from their successes and failures — over a myriad experiences and environments," Cunningham said.

The LDP selected books from the Skillport e-learning portal and facilitated sessions for up to 30 DCSA employees. Feedback has been overwhelmingly positive, and participants remarked that the selected books introduced them to concepts they had not previously considered.

"I learned the importance of creating a personal connection when initiating a conversation. More importantly, even if we don't feel a connection, don't take it too personally. Use that as a learning experience to make the conversation go a little better the next time!" **— Karin Moya, HCMO**

Bonny Boltz, branch chief of the Department of Defense Consolidated Adjudications Facility (DoD CAF) also reported valuable leadership best practices, "The sharing and exchanging of ideas and situations fostered out-of-the-box thinking and encouraged new ways of approaching a problem in leading," said Boltz. "I learned that, to be effective, those in charge must give their team a reason to follow them and work together. Building trust, driving results, and winning respect can be accomplished by doing simple things every day to give your team a reason to believe in and follow your guidance."

Jodi Weaver from the Background Investigations Customer and Stakeholder Engagement Division appreciated explicit team building techniques and real-world examples. "It was great to hear real-life examples from other members of our organization about leadership strategies that have had a positive outcome in their experience," said Weaver. "In addition, the book itself provided many examples of how other leaders have changed the outcome of certain situations by utilizing various leadership techniques, which include empowering their team members by involving them in the decision-making process."

"The leadership book club with Larry Cunningham made me a better leader. Not only as a field investigator — I am a better all-around person for it." **— Kevin Arnett, Background Investigations Division, Indianapolis Field Office**

WHAT WE'RE READING:

- **"Eisenhower on Leadership: Ike's Enduring Lessons in Total Victory Management"** by Alan Axelrod
- **"Become: The Path to Purposeful Leadership"** by Mark Hannum
- **"Everyone Communicates, Few Connect: What the Most Effective People Do Differently"** by John C. Maxwell
- **"The 21 Irrefutable Laws of Leadership: Follow Them and People Will Follow You"** also by John C. Maxwell
- **"Lead by Example: 50 Ways Great Leaders Inspire Results"** by John Baldoni

MY EXPERIENCE IN THE DCSA LEADERSHIP DEVELOPMENT PROGRAM

By Alexander Merriam
Critical Technology Protection

When I started the Leadership Development Program (LDP) in the summer of 2019, I did not appear to be the poster child for a leader. I was a 23-year-old GG-9 with less than two years of federal service. However, in my relatively short time with the government, I have learned to never say no to an opportunity for training.

I participated in a unique iteration of the LDP, as it was the first one that included employees from outside of the then-Defense Security Service (DSS) with participants from the Department of Defense Consolidated Adjudications Facility (DoD CAF). My team included Alexa Gunsell, an adjudicator from DoD CAF; Robert Ranker, a counterintelligence special agent (CISA); Robert Riggle, a former information system security professional (ISSP); Garrett Speace, a senior industrial security representative (ISR); and a current network manager within Office of the Chief Information Officer (OCIO). Our assigned capstone project topic was industry supply chain monitoring.

The LDP facilitated and guided participants to identify their own individual strengths and weaknesses via a self-assessment, as well as a "360 assessment" completed by our peers and supervisors. Additionally, the LDP allowed participants to develop soft skills that are crucial to effectively performing our duties as public servants, while complementing hard skills applicable to our individual positions. Professionals such as Dr. Fred Bolton and Larry Cunningham from DCSA's Human Capital Management Office (HCMO), as well as representatives from the Center for Creative Leadership, facilitated trainings such as conflict resolution, public speaking, communication, delegation, prioritization, self-help, teamwork, integrity, and many more. These lessons and activities were conducted virtually and in-person.

Like any other learning opportunity worth your time, my experience in the LDP was not without its challenges. The Office of General Counsel deemed our capstone topic's initial goal to be out of the scope of DCSA's current authorities. As a result, our group had to pivot to achieve our goal, while remaining in compliance with the laws and regulations in place at the time. Our topic directly related to my day-to-day duties as an ISR, which was not only beneficial to furthering my own professional development, it helped my team members learn about DCSA activities outside of their normal duties.

The LDP experience allowed our group one-on-one facetime with senior leaders who delivered candid and overwhelmingly positive feedback. One of the more significant challenges was getting to know each other personally and professionally while working across three time zones. Fortunately, the group came together quickly, and friendships developed as we completed our capstone project. I am proud of the work that our group accomplished and the connections we forged over the course of the nine-month program. I would highly recommend the LDP to any DCSA employee, no matter their grade level or leadership experience. We all have the opportunity to learn.

(Working through the Leadership Development Program experience were (from left to right) Robert Riggle, Office of the Chief Information Officer; Alexander Merriam and Garrett Speace, Critical Technology Protection; Robert Ranker, Counterintelligence Directorate; and Alexa Gunsell, DoD CAF.)

COMMITTED
TO MISSION

PASSIONATE
ABOUT SERVICE

UNWAVERING
IN INTEGRITY

DRIVEN
TO INNOVATE

INVESTED
IN PEOPLE

Defense Counterintelligence and Security Agency

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil

571-305-6562

www.dcsa.mil