DCSACCESS

Official Magazine of the Defense Counterintelligence and Security Agency

Volume 9, Issue 4

AMERICA'S GATEKEEPER

A Day in the Life: Firsthand Accounts from the Field

DCSA Marks One-Year Anniversary and Looks Ahead

Cogswell 2020: DCSA Recognizes the Best in Industrial Security

IN THIS ISSUE

VOL 9 | ISSUE 4

DCSA ACCESS

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

FROM THE DIRECTOR

This issue of the ACCESS is special because it provides a snapshot of DCSA's expanded mission as we pass the one year mark for the creation of the new DCSA. We also honor the recipients of the 2020 Cogswell Award as well as highlight the diverse and expanded mission sets across the agency and the employees who are performing them.

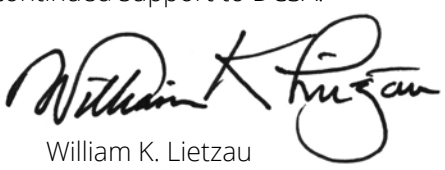
Due to COVID-19 restrictions, the Cogswell presentations — normally held at the annual NCMS training event — were instead handled virtually. Although the event was scaled back, the commitment, dedication, and outstanding work exhibited by the recipients was not diminished in any way. The Cogswell Award continues to recognize the pinnacle of industrial security excellence and the enduring partnership between DCSA and industry. In keeping with past tradition, we invited several of the winners to share the secret to their success in their own words. I think you will find their stories compelling, and I hope they will serve as a model for others to emulate. Instilling a culture of security is often our best protection from the extant and growing threat from our potential adversaries. Congratulations to all our Cogswell Award recipients for 2020.

October 1, 2020, marks one year since DCSA assumed the background investigation mission from the Office of Personnel Management's (OPM) National Background Investigations Bureau (NBIB) as well as the adjudication mission from Washington Headquarters Service's DoD Consolidated Adjudication Facility. The most recent transfer included more than 3,300 civilian employees, 2,000 vehicles, 37 active contracts, and the establishment of a new working capital fund. All this took place while DCSA continued stabilizing both the investigative and adjudication inventories and fulfilling an increasingly important role overseeing the National Industrial Security Program (NISP).

The breadth and diversity of the DCSA mission is impressive. This issue highlights what it means to work in DCSA's various security disciplines from investigators to industrial security representatives and counterintelligence special agents and analysts. We have people across the country working under difficult circumstances, dedicated to and focused on missions that could not be more important. Their first-hand accounts are both interesting and inspiring.

Reflecting on how far we have come is important, but there is simply no time for us to rest on our laurels. This October, DCSA will again welcome new employees and missions from OPM, the Defense Manpower Data Center (DMDC), the Defense Intelligence Agency (DIA), and the Defense Information Systems Agency (DISA). Once these final transfers are completed, DCSA will continue to transform as we integrate our new components. It is an exciting time for DCSA, and I look forward to sharing more of our journey in future issues.

Thank you for reading and for your continued support to DCSA.

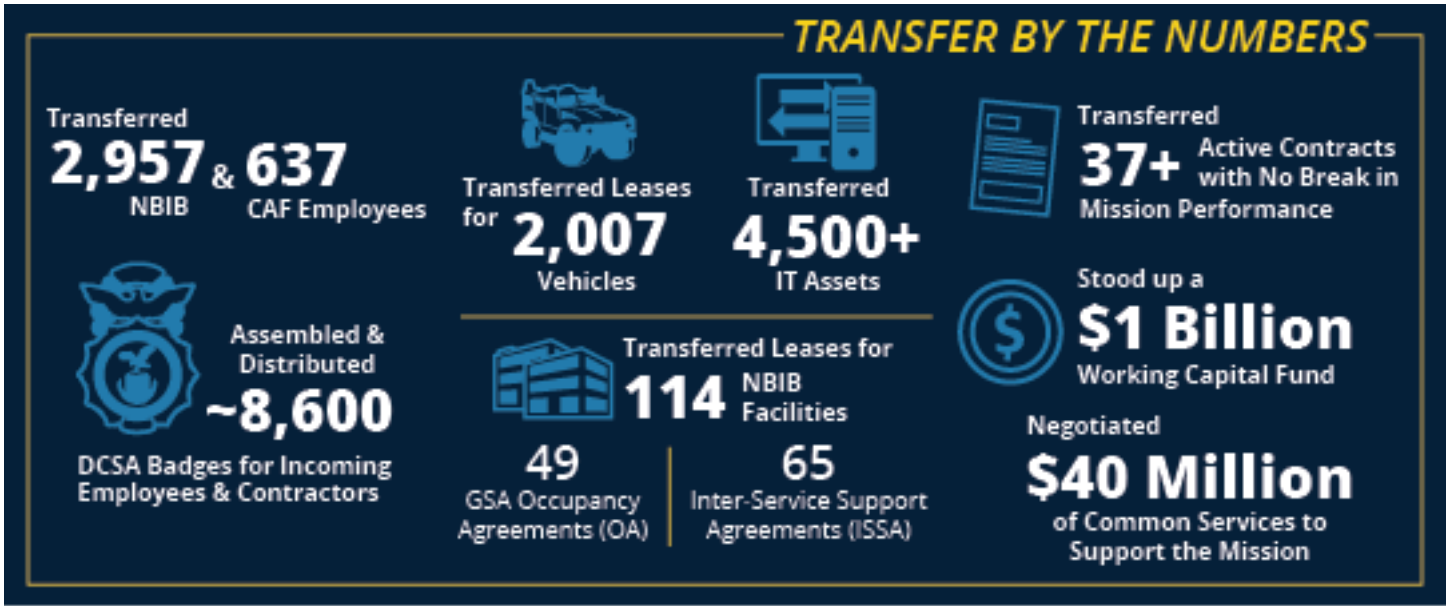


William K. Lietzau

Director,
Defense Counterintelligence
and Security Agency

DCSA MARKS ONE-YEAR ANNIVERSARY AND LOOKS AHEAD

On October 1, 2019, the Defense Counterintelligence and Security Agency (DCSA) became the largest security agency in the federal government with the mission of ensuring the trustworthiness of the United States government's workforce, the integrity of its cleared contractor support, and the uncompromised nature of its technologies, services, and supply chains. DCSA resulted from the consolidation of the National Background Investigations Bureau (NBIB), the DoD Consolidated Adjudications Facility (DoD CAF), and the Defense Security Service (DSS).



While DCSA has achieved much in the past year, change continues to define the agency. This October, DCSA is poised for another set of transfers that will make DCSA the custodians of the largest personnel security IT systems in the federal government. On January 28, 2019, a memorandum issued by Deputy Secretary of Defense David L. Norquist directed the move of the National Background Investigation Services (NBIS) Program Executive Office (PEO) from the Defense Information Systems Agency (DISA) to DCSA. NBIS is a new enterprise-wide information technology (IT) system that is transforming the personnel vetting process to deliver stronger security, more customizable solutions, faster processing, and reduced cost while also enhancing the user experience.

The same memorandum directed the transfer of personnel vetting systems and associated functions, personnel, and resources supporting the Defense Vetting Enterprise from the Defense Manpower Data Center (DMDC) and the DoD Human Resources Activity (DHRA). These vetting systems include the Defense Information System for Security (DISS), Joint Adjudication Personnel System (JPAS) as it is decommissioned, the Defense Central Index of Investigations (DCII), MIRADOR (the records system for Continuous Evaluation), the Secure Web Fingerprint Transmission (SWFT) System, and the Individual Investigative Records Repository (IIRR).

And finally, DCSA will assume responsibility for the maintenance and operation of the following legacy IT systems from the Office of Personnel Management (OPM): the Personnel Investigations Processing System (PIPS) and related personnel vetting IT systems such as the Central Verification System (CVS), OPM PIPS Imaging System (OPIS), e-Delivery, Fingerprint Transaction Systems (FTS), Field Work Systems (FWS), Non Field Work Systems (NFW), NP2, and the Dashboard Management Reporting System (DMRS).

IN TOTAL, THE TRANSFER WILL INCLUDE:

Defense Information Systems Agency (DISA): National Background Investigation Services (NBIS) IT systems and Joint Services Provider (JSP).

Defense Manpower Data Center (DMDC): Personnel vetting systems including: Defense Information System for Security (DISS), MIRADOR (the Continuous Evaluation records system), Secure Web Fingerprint Transmission (SWFT), Individual Investigative Records Repository (IIRR), and Defense Central Index of Investigations (DCII).

Defense Intelligence Agency (DIA): Operational control of National Center for Credibility Assessment (NCCA) and Executive Agent for Security of DoD Personnel at U.S. Missions Abroad. Full programmatic transfer on October 1, 2021.

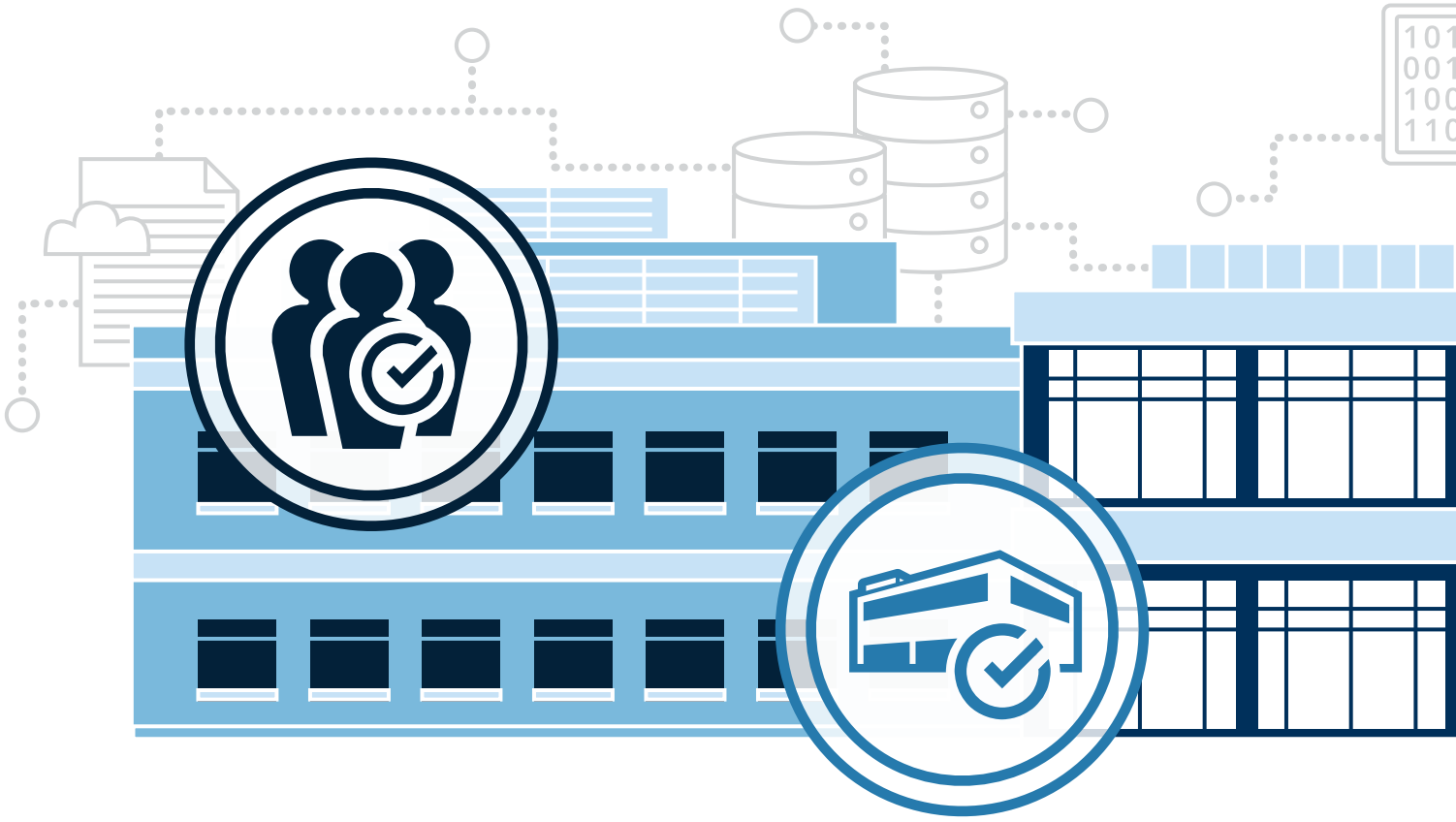
Office of Personnel Management (OPM) Financial Management (FM) and Information Technology (IT): Financial data and legacy personnel vetting IT capabilities: the Electronic Questionnaires for Investigations Processing (e-QIP), Position Designation Tool (PDT), and Personnel Investigations Processing System (PIPS), as well as the Central Verification System (CVS), OPM PIPS Imaging System (OPIS), Dashboard Management Reporting System (DMRS), Fingerprint Transaction Systems (FTS), NP2, Field Work System (FWS), Non Field Work System (NFW).

With so many disparate elements coming together under the DCSA umbrella, it's important that DCSA stakeholders and employees alike understand what each mission area and office does and how it all relates to each other. It's been said that you can't truly understand a person until you've walked a mile in their shoes. In the following pages we've tried to capture just that — what it's like to be an adjudicator, a background investigator, an industrial security representative, a counterintelligence special agent. Through these personal stories, we hope to offer a glimpse into the depth and breadth of the agency and the challenges the DCSA workforce faces in completing them. These personal stories will continue into the January issue as the "Day in the Life" series becomes a standing feature of ACCESS Magazine.

DCSA AT A GLANCE

DCSA is our nation's gatekeeper. On October 1, 2019, DCSA became the security agency in the federal government dedicated to securing the trustworthiness of the United States government's workforce and the integrity of its cleared contractor support, technologies, services, and supply chains. Through personnel vetting, industrial security engagement, counterintelligence support, and education and training, DCSA's combined mission capabilities deliver optimum performance in protecting our nation's security.

DCSA'S MISSION

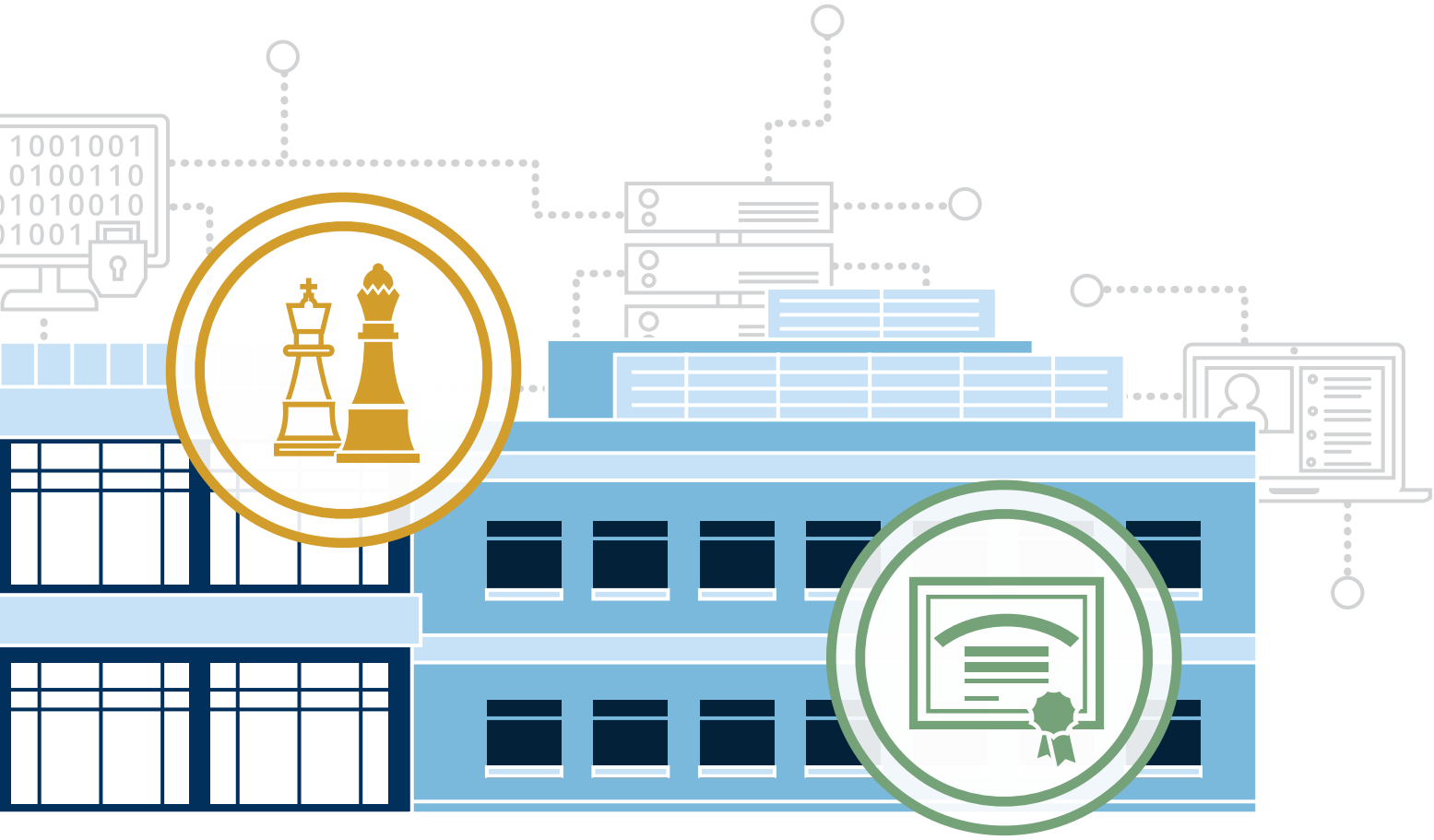


PERSONNEL VETTING

DCSA is the primary investigative service provider (ISP) for the federal government, delivering efficient and effective background investigations for 105 government departments and agencies. DCSA also adjudicates clearance requests and is at the forefront of developing a Continuous Vetting program that will safeguard the integrity and trustworthiness of the federal and contractor workforce.

CRITICAL TECHNOLOGY PROTECTION

DCSA provides oversight to 12,500 cleared facilities in the National Industrial Security Program (NISP), ensuring that the sensitive and classified U.S. government information that contractors are entrusted with, and the critical technologies they develop, are properly protected.



COUNTERINTELLIGENCE

DCSA's Counterintelligence mission is the federal government's strongest link between the nation's industrial base, the U.S. Counterintelligence (CI) and Intelligence Community (IC), and federal law enforcement (LE). It leverages collection of CI threat information against our cleared workforce and critical technologies to inform robust analysis and production of intelligence products shared across the IC/LE community.

NATIONAL SECURITY LEARNING CENTER

DCSA is comprised of three educational institutions, the Center for Development of Security Excellence (CDSE), the National Training Center (NTC), and — as of October 1, 2020 — the National Center for Credibility Assessment (NCCA), which provide development, delivery, and exchange of security knowledge to ensure a high-performing workforce.

PROTECTING AMERICA'S CRITICAL TECHNOLOGY

DCSA's Industrial Security Directorate provides oversight to approximately 12,500 cleared facilities in the National Industrial Security Program (NISP), ensuring that the sensitive and classified U.S. government information that contractors are entrusted with, and the critical technologies they develop, are properly protected.

The NISP was established by Executive Order 12829 to ensure U.S. cleared industry safeguards classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. DCSA administers the NISP on behalf of the Department of Defense (DoD) and 33 other federal agencies, making sure they are compliant with the NISP Operating Manual (NISPOM).

A HOLISTIC LOOK AT SECURITY

DCSA takes a holistic approach to security within the NISP, making sure facilities, personnel, and associated IT systems are safeguarded from attack and fully in line with the NISPOM.

FACILITY CLEARANCES

DCSA processes, issues, and monitors eligibility of facility clearances (FCL) for companies that require access to classified information. An FCL is the determination that an entity, including a company or an academic institution, is eligible for access to classified information or award of a classified contract.

Once an FCL is granted, DCSA has oversight authority to evaluate the security operations of the organization. An industrial security representative (ISR) acts as the principal interface with the contractor's facility security officer (FSO) and management staff.

ACCESS ELSEWHERE FACILITIES

For select companies that do not access classified information onsite (approximately 60%), DCSA will conduct an assessment of their security program to determine which facilities meet the criteria to transfer to the **National Access Elsewhere Security Oversight Center (NAESOC)** for centralized and consolidated support. By separating oversight of possessing and non-possessing facilities, DCSA can provide better support to both, while better protecting the critical technologies vital to national security.

INFORMATION SYSTEMS

DCSA handles Assessment & Authorization (A&A) determinations for the National Institutes of Standards and Technology (NIST) Risk Management Framework (RMF), a common set of guidelines and minimum requirements for classified information systems. Using the DCSA Assessment and Authorization Process Manual (DAAPM), DCSA's information system security professionals (ISSP) work hand-in-hand with ISRs and other DCSA field staff to assess industry's cybersecurity risk management processes. DCSA uses Enterprise Mission Assurance Support Service (eMASS) for authorization decisions, a web-based database for comprehensive and integrated cybersecurity management that allows for reporting and facility scoring with strict process control mechanisms.

INDUSTRIAL SECURITY BY THE NUMBERS

45 Field Offices

550 Employees & Contractors

33 NISP Signatories

12,500 Cleared Facilities

FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI)

A company is considered under FOCI whenever a foreign interest has power over the company — direct or indirect — that could result in unauthorized access to classified information or adversely affect a classified contract's performance. DCSA's Entity Vetting unit works with ISRs to analyze and mitigate any FOCI concerns for facilities that work with classified information. FOCI specialists perform a holistic review of each facility and the ownership structure, ensuring they are able to secure and protect classified information without affecting national security.

SPECIAL ACCESS PROGRAMS

Special Access Programs (SAPs) are designed to provide enhanced security measures to protect the United States' most critical and sensitive capabilities, technologies, information, and operations. DCSA SAP specialists work with ISRs and ISSPs and the government contracting agencies (GCA) to ensure a contractor is meeting its security requirements.

LIAISING ACROSS DCSA

PERSONNEL

The security of industry's cleared facilities is only as strong as the people protecting it. The Industrial Security Directorate works closely with the Personnel Vetting mission to ensure industry's FSOs and security managers have the resources they need.

COUNTERINTELLIGENCE

The Industrial Security Directorate works hand-in-hand with DCSA's Counterintelligence (CI) program to identify and mitigate attempts by our nation's adversaries to steal sensitive national security information and technologies from cleared industry. DCSA then works with companies to better protect the assets, identify vulnerabilities, and apply CI threat information.

A DAY IN THE LIFE: INDUSTRIAL SECURITY

CURTIS PEAY, KATY LIMON, AND LAHOMA KOTCHIAN

Senior Action Officers, Western Region

Q: What does an SAO do?

A: As senior action officers (SAOs), we are subject matter experts on the National Industrial Security Program (NISP), providing oversight and security education to DCSA industrial security personnel and industry partners. We act as a liaison between headquarters and field elements, ensuring policy is communicated down, while vulnerabilities and risks are communicated up. We help the industrial security representatives (ISRs) in the field mitigate complex security threats at the facilities they oversee. Often former ISRs ourselves, SAOs utilize their on-the-ground experience when providing the field with actionable assistance.

Three or four action officers support each region. In our region, each action officer is assigned oversight and assistance to approximately two field offices (there are six field offices in Western Region). SAOs work behind the scenes to keep the ships going. Nearly half of the day can be spent resolving a multitude of issues, ranging from running a quality check on a Critical Communication & Coordination Tool (3CT) that received a recommendation for an unsatisfactory rating, to analyzing a complicated business structure for a new facility clearance application package, or reviewing a foreign ownership, control, or influence (FOCI) mitigation plan and supplemental plans.

When the action officer position was created in each region in 2008, we were known as FOCI/international specialists, and we specialized only in those areas. Now, we handle a variety of issues as well as assist with FOCI and international security concerns. Ultimately, we have to make sure that we are up to date with any industrial security policy and procedure changes to be able to arm field personnel with the knowledge and resources they need.

Typically, our workflow starts when an ISR or field office chief contacts us with an issue or when a task that requires our review comes down from headquarters. Depending on the situation, it can take anywhere from a week to several years to finalize an issue since there are a number of internal and external parties that must be on the same page before it's resolved.

We provide training, as needed, share knowledge through mentoring opportunities, and participate in diverse working groups to advance DCSA's mission, capitalize on lessons learned, and improve processes for the future. We also report a variety of high-impact, risk-related issues, typically developed in the field, to headquarters through the internal "What Everyone Should Know" (WESK) report, some of which is passed up to relevant agencies within DoD in the "Weekly Operational Activity" report (WOAR). At the same time, we report back to ISRs and the field offices on which critical technologies and potential risk factors need to be prioritized when assessing facilities.

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

A: Keeping pace with changes in industrial security policy and procedures is by far the most challenging aspect of our jobs. Being a good researcher and knowing where and who to go to for help is the key to our position. We are expected to be subject matter experts on everything, and not being in the field every day can make it more challenging. Keeping up with information and managing the volume of work within a constantly evolving field can be difficult as well.

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

A: This is a diverse job where each day you're presented with a new challenge. The ability to always find something new to learn is incredible and being able to build relationships at both the field and headquarters level is great.

DEBORAH DRAKE

Junior Industrial Security Representative, Southern Region

Q: What does an ISR do?

A: I am an industrial security representative (ISR) in the Huntsville, Alabama Field Office. My job is to support cleared industry's ability to deliver uncompromised products and services to the U.S. government. But I can't do that without first making sure that they're trustworthy and that they have the proper security measures in place. An ISR may have 100 or more facilities of various sizes and complexities assigned at one time. We work with each facility to move through the process of obtaining a facility clearance (FCL) and continue providing support once the FCL is granted.

I do regular security assessments throughout the year to ensure that facilities are protecting the information they have access to. During the assessments, I physically go in and ensure that they are adhering to the National Industrial Security Program Operating Manual (NISPOM), the operating manual for companies within the National Industrial Security Program (NISP). It also lays out requirements and safeguards needed to protect classified information. I do both onsite assessments as well as several virtual or telephone meetings throughout the year. I will make sure they are protecting classified information within their possession and verify they have proper safeguards in place.

> *"As an ISR, we're the direct link between the agency and industry."*

For facilities that have been newly granted FCLs, we perform mock assessments, called Initial Compliance Contact (ICC) engagements, to make sure they are on track with understanding and meeting NISPOM requirements 120 days after the initial FCL has been granted. We then perform a formal Enhanced Security Vulnerability Assessment (ESVA) after one year. Before and after an assessment, we continuously engage with facilities to answer any questions they may have or assist with the investigation of security violations throughout the year.

The most time-consuming part of the job for me is when my facilities have questions about how to meet certain requirements. There are so many different scenarios that you run into when dealing with security at this level. I have facilities call with questions about personnel security requirements, safeguarding classified information, managing classified information systems, investigating potential security violations, understanding foreign ownership, control, or influence (FOCI), and identifying perceived security threats. A lot of the work for me is understanding that each of these situations is different. While I do have specific NISPOM and internal guidelines that outline each of those requirements, I need to be able to understand the specific situation that's going on in that facility and think through our risk-based approach to give a response that fits their true circumstances.

As an ISR, we're the direct link between the agency and industry. We are allowed face-to-face interaction with facilities to understand how policies immediately impact them. If you don't get that direct face-to-face interaction, as it is in some other areas of the agency, I imagine it's a lot easier to feel a divide between government's and industry's goals.

Q: How does an ISR support DCSA's mission?

A: Our mission is to support industry's ability to deliver uncompromised technology and services. As an ISR, I get the opportunity to understand how facilities are adhering to security requirements and how these requirements immediately impact them. We also continue to support DCSA by ensuring facilities not only understand what our mission is, but also understand the intent behind our policies and the impact of failing to adhere to these policies. I feel like we get to do that on a more personal level and that makes a big difference to me.

Q: What is your favorite part of the job?

A: What I really enjoy about working in this position is understanding that ISRs will never know all the answers to every question, no matter how many years they have been in the career field. There's always something new to discover, to research, to learn. And there's no possibility to get bored, because everything changes from day to day. The agency as a whole is evolving so quickly. There are so many opportunities for advancement — I just want to be a part of all of it. I'm very interested in continuing to see how our mission expands and how we as an agency grow to meet the ever-changing demands to maintain national security.

KEVIN MCPHERSON

Senior Industrial Security Representative, Industrial Security Directorate, Capital Region

Q: What does an ISR do?

A: As an industrial security representative (ISR), I serve as the primary interface between the U.S. government and industry. I work to ensure facilities in possession of or access to classified information and critical technologies comply with the National Industrial Security Program (NISP) through the NISP Operating Manual (NISPOM), the manual that prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information for companies within the NISP.

We review how classified information comes into the facility, who touches the information, who has access, what someone is doing with that information, and what happens when the facility turns over the classified information to the government agency that owns it. It's a daily interaction of fielding questions, providing guidance, and performing security briefings to ensure that a facility's interpretation of a particular policy is conforming with government's interpretation.

Part of the job calls for me to go out to these facilities for periodic security reviews. When I'm onsite, I usually start by sitting down with leadership to talk about how their facility is meeting the necessary security requirements. This can be executives from Fortune 500 companies or smaller mom-and-pop shops. The other side of my job is fielding questions. I get calls at all hours ranging from a company calling to ask me where to store their government equipment because their facility flooded, to someone asking if they can use a classified Secret CD in their personal computer, to which the answer is always no because it's classified.

> *"My favorite part about being an ISR is being out in the field and seeing the technology that is going out to the warfighter.*

Depending on the size and scope of the review, I coordinate with information systems security professionals (ISSP) and counterintelligence special agents (CISA), and often headquarters in the case of international programs or foreign ownership, control, or influence (FOCI). Whether I am conducting a review or performing continuous monitoring, I like to ensure I have insight on what threats are out there, so I rely on CI to share that information. For example, if a facility receives a suspicious email with suspicious links or attachments, the company will contact me on how to report the email. I provide clear instructions on submitting the email to CI so not to potentially infect DCSA networks with malware. They review for potential bad actor information and report that out as necessary. Similarly, I have to have a good working relationship with ISSPs so we can share information openly in the event of a data spill to ensure the facility adequately sanitized any systems.

I typically oversee over 70 companies. Senior ISRs are assigned the larger and more complicated facilities that deal with issues such as FOCI or a facility campus that encompasses multiple buildings with thousands of employees. Senior ISRs also provide guidance when a junior rep encounters an unfamiliar scenario. We share information and best practices and act as a lead advisor during training and ride-alongs.

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

A: The most challenging aspect of my job is probably sifting through the noise to make sense of all the data coming through. This job is really about being flexible and quick to adapt. I've gotten calls at 3:30 p.m. on a Friday about a company that just experienced a major data spill. Calls can come at any time, so ultimately, it comes down to being well-informed in threat research. An analytical background is essential as well as building communications skills and adapting to the changing threat environment within the industrial security field.

We are also always innovating our methodologies to be more efficient and better protect against risk. At the same time, I'm learning new ways of doing business, I need to teach my facility security officer (FSO) counterparts in industry how to think beyond just checking the boxes, to really think in a risk-based approach.

Q: What are the most rewarding factors of your job?

A: I enjoy being at the forefront of critical technology protection. My favorite part about being an ISR is being out in the field and seeing the technology that is going out to the warfighter. It's amazing seeing the technology come off the assembly line, knowing how many years of effort went into it. I think if we, the 160 ISRs of DCSA, were not out in the field doing security oversight, I don't think we would be as successful in making sure industry is protecting classified information and national security.

LUCY RODRIGUES

Senior Information Systems Security Professional, NISP Authorization Office

Q: What does a Senior ISSP in the NAO do?

A: I am an information systems security professional (ISSP) for the NAO, the DCSA office that manages Assessment & Authorization (A&A) for the National Institutes of Standards and Technology's (NIST) Risk Management Framework (RMF), which is a common set of guidelines for securing classified systems.

Before the framework was established, each federal agency used different methods of assessing and authorizing classified information systems, which became an issue for information sharing and reciprocity across agencies. The RMF established this common set of guidelines, required by law, and provides instructions to secure operation of systems processing classified information.

Our goal is to enhance industry's ability to securely configure classified systems, get them authorized, and provide the quality assurance and support they need. My primary role is making sure everyone understands our policies and our process by developing and maintaining the DCSA Assessment and Authorization Process Manual (DAAPM), as well as job aids and operation guides not only for industry but also for our personnel in the field.

On a typical day, I am continually developing and improving internal and external guidance to better provide solutions that ensure security, risk mitigation, and safeguarding of classified information. I provide operational support to industry and the field personnel by providing guidance related to RMF, policy changes, and the Enterprise Mission Assurance Support Service (eMASS), the new database of record for A&A activities and integrated cybersecurity management.

I'm also one of the two NAO staff members who manages the NISP's eMASS. The NISP instance of eMASS is the largest in the country with over 3,000 users and over 6,000 registered information systems. As one of the primary NAO staff members managing the NISP eMASS, I'm responsible for managing system development, operations, and account management. I provide training, troubleshooting, and answer questions regarding the application. The focus is to give people the guidance they need to do their jobs, and that means supporting our industry partners and our internal personnel executing the assessment and authorization process.

Q: What's unique about your job that most people might not know?

A: My job never stays the same. Developing eMASS and ensuring its functionality has been a constant challenge for the past year, but it's been a rewarding experience. First, it was establishing our instance of eMASS and developing operational guides and processes. Then, it was setting up user accounts and guiding industry through the process of registering systems. And now, we are constantly evaluating and troubleshooting — every day is new for me. I know I can never truly be a subject matter expert on any one thing because it changes so much. But that's the great part, I'm constantly researching and learning something new every day. I can't say that I've ever had a boring day with NAO.

Q: What drew you to this career path?

A: I was an information systems technician in the U.S. Navy and transitioned as a civilian working for a research and development facility in Boston. While working there, I met DCSA's assigned ISSP, who came to perform an assessment at my facility. I worked well with my assigned ISSP and became very curious about the agency. I said to myself, "I'd love to work for the government," and went to the USAJobs website, applied, and got hired. I started as an ISSP in the Boston Field Office and then was promoted to ISSP team lead. Then about five years ago, I got this amazing opportunity to work for NAO. I enjoy my job. I really love working for DCSA because of the mission, and the people are just incredible.

Q: What is it about your job that helps DCSA complete its mission?

A: My role ensures consistent policy implementation, training, and providing resources. Assessment & Authorization isn't the only piece of the puzzle, but it's my part in supporting the mission. We're overseeing the execution of the A&A process within the NISP, and it's our responsibility to make sure that policy implementation is correct. We provide that oversight and ensure that information is protected, that industry is aware of their responsibilities, and that our internal personnel get the support and resources and guidance to do their jobs.

January's ACCESS will feature more firsthand accounts from DCSA's Industrial Security Directorate.

PERSONNEL VETTING: SECURING THE TRUSTWORTHINESS OF THE WORKFORCE

DCSA's Personnel Vetting mission delivers efficient and effective background investigations, adjudications, and DoD's continuous vetting services to safeguard the integrity and trustworthiness of the federal and contractor workforce.

PERSONNEL VETTING BY THE NUMBERS

2.6M
Federal Government Background Investigations Annually

1M
Federal Government Adjudications Annually

105
Departments & Agencies

2.3M
Enrolled in the Continuous Evaluation Program

STEPS OF THE PERSONNEL VETTING PROCESS

BACKGROUND INVESTIGATIONS

DCSA's background investigations are the first step in the personnel vetting process. As the primary investigations service provider (ISP), DCSA conducts background investigations for 95% of the federal government. This includes not just security clearances for access to classified information, but also suitability determinations for non-sensitive positions. DCSA follows a "whole person" approach, which ensures every person is evaluated based on the sum total of their character, trustworthiness, loyalty, and ability to protect classified investigations. Investigators rely on automated records checks and in-depth interviews pertaining to applicants to conduct background investigations.

INVESTIGATION REVIEW

From start to finish, quality is built into every step of the background investigation's review process. DCSA's Federal Investigative Records Enterprise (FIRE) office maximizes the exchange of information and optimizes business operations by automating the management, collection, and retention of investigative records in a digitized platform. This promotes effective communication between DCSA and its partners, including other federal agencies, state and local entities, and commercial records providers.

At the same time, DCSA's Quality Oversight team performs a thorough evaluation to detect potential disqualifying information, counterintelligence concerns, and insider threats before adjudication. They also provide quality assurance and integrity measures to validate an investigators' source information. This wholesale approach works to ensure the integrity and trustworthiness of the federal and contractor workforce.

ADJUDICATIONS

DCSA's Department of Defense Consolidated Adjudications Facility (DoD CAF) adjudicates, or determines, the clearance eligibility of non-Intelligence agency DoD personnel occupying sensitive positions and/or requiring access to classified material. The DoD CAF customer base also includes members of Congress, the Congressional Budget Office, the United States Capitol Police, selected judicial staff, DoD personnel at the White House, and contractor personnel under the National Industrial Security Program (NISP).

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 personnel eligibility to access national security information. The CAF also renders certain suitability, fitness, and credentialing determinations.

SECURITY CLEARANCE ELIGIBILITY

A security clearance eligibility is a determination that a person is able and willing to safeguard classified national security information and/or occupy a national security sensitive position. The three national security clearance eligibility levels are: Confidential, Secret, and Top Secret.

SUITABILITY/FITNESS

Suitability is the determination of whether or not a person's character or conduct is in line for competitive federal service and senior executive service positions. Similar to suitability guidelines, fitness decisions are made for excepted service, contractor, and other federal personnel.

CREDENTIALING

The credentialing process determines whether or not to grant individuals access to federal property and information systems. The Homeland Security Presidential Directive-12 program provides guidance for issuing Common Access Cards (CAC) and Personal Identification Verification (PIV) cards.

CONTINUOUS VETTING

In conjunction with the federal government's background investigation reform effort, DCSA is developing a Continuous Vetting (CV) model to mitigate vulnerabilities in real time. This move entails regularly reviewing cleared individuals' background to ensure they continue to meet security clearance requirements, ultimately enhancing the timeliness and quality of background investigations. The program is supported by Continuous Evaluation (CE), a set of automated record checks that pulls data from criminal and financial databases, as well as public records, at any time during an individual's period of eligibility.

INSIDER THREATS

The DoD Insider Threat Management & Analysis Center (DITMAC) coordinates with 44 insider threat hubs across DoD and the military services to better share information in one integrated platform. The goal of DITMAC is to mitigate insider threat risks before violence or unauthorized disclosures occur. DITMAC's subject matter experts collaborate with the hubs on an appropriate response, treating risk not just from a security perspective, but a whole-of-person perspective. Subject matter experts include law enforcement, counterintelligence, cyber, and behavioral scientists.

BACKGROUND INVESTIGATIONS MISSION ACHIEVES, SUSTAINS MANAGEABLE INVENTORY

By Collette Khajehali
Background Investigations Front Office

After an intense, collaborative effort, the Background Investigations (BI) mission achieved a manageable inventory of 200,000 cases in mid-April. And in May, for the first time since spring 2014, DCSA met the Intelligence Reform and Terrorism Prevention Act (IRTPA) investigative timeliness requirements for Top Secret (T5) initial investigations and decreased Secret (T3) investigations timeframes by more than 73%, nearing its 40-day goal while maintaining a 99% quality rating.

This achievement comes after the BI mission's case inventory peaked at 725,000 cases in April 2018. The main cause of the accumulation was due to the loss of a National Background Investigations Bureau (NBIB) contractor in September 2014, which accounted for the majority of the investigative capacity across the enterprise. The lack of manpower — combined with needing to implement the 2012 Federal Investigative Standards (FIS) and a massive increase in the number of investigations submitted — created a "perfect storm." The case inventory almost tripled that of its usual, optimally functional volume. Senior leaders across the executive and legislative branches, industrial partners, and the media identified this issue as a government-wide crisis, many calling for swift action to reduce the inventory.

In collaboration with the executive agents — the Office of the Director of National Intelligence (ODNI) and the Office of Personnel Management (OPM) — the BI mission used a multifaceted, phased approach to reduce the backlog, including:

- Re-engineering business processes (e.g., leveraging technology, centralizing workloads, etc.).
- Increasing the federal and contract investigative workforce by more than 50%.
- Informing policy makers in making necessary changes to personnel vetting policies.
- Leveraging the hard work of its dedicated workforce.

Ultimately, the BI mission achieved its goal of a manageable inventory that keep investigations flowing through the system to produce high-quality, cost-effective investigations in a timely manner and balances the number of trained investigators on hand, projected volume of cases submitted by agencies, policy requirements, processes, and information technology capabilities. These major accomplishments — both reducing and sustaining the inventory by more than half a million cases — have received public acknowledgment and accolades from the mission's customer agencies, industry partners, Congress, and the highest levels of the executive branch.

While achieving a manageable inventory, the BI mission now faced the challenge of a global pandemic with COVID-19, which resulted in wide-spread impacts to the BI mission and its operations on various levels. Propelled by a spirit of partnership across the Personnel Vetting mission and its components, DCSA took immediate action to ensure the safety of the workforce and continuity of operations. This included implementing maximum telework, issuing operational guidance to allow for alternative investigative methodologies, approving capabilities to conduct virtual interviews, and altering IT systems to expand virtual case processing. The pandemic continues to require partnership, open-mindedness, and an "all hands on deck" attitude to maintain recent successes on timeliness, which are a critical success factor for the mission and vital to national security.

To learn more about background investigations, read the following articles for employees' firsthand accounts of their jobs and how they relate to the DCSA mission.

A DAY IN THE LIFE:
BACKGROUND INVESTIGATION

WILFREDO "WILLIE" RAPOPORT

Assistant Regional Director, Western Region

Q: What is a typical day like for you?

A: As an assistant regional director, there is no such thing as a typical day. I'm in a management position — a supervisor of supervisors — and I am responsible for eight special agents-in charge (SACs) and field offices with more than 100 field personnel. My business is people. I make sure folks are taken care of, i.e. payroll, morale/employee issues, and getting information out. Sometimes my day is focused on employee relations, while other times I'm focused on more operational concerns like productivity. I'm also thinking of our 30-60-90-day outlooks to determine what will be needed or what changes we can make to do better.

> *"The field workforce has continued this incredible job through COVID operations. I have always been proud of our ability to be flexible and adapt, and this period of time has been no different. Our teams are getting the mission done and are doing it well.*

Q: What are some of your responsibilities when it comes to the operational side of the business?

A: For most of the last three years, my operational focus has been on production and productivity — basically, the time from when cases are "fielded" to when they are completed. Now that we're not operating with an overwhelming inventory of cases, we have shifted from efficient production as the primary focus to getting cases done in a timely manner without loss of efficiency.

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

A: We have one mission: conduct the background investigation with a complete picture to enable an informed adjudicative decision. We do this by conducting effective interviews, reviewing records in an informed way, and following up as issues develop. I think one of the ways I personally contribute to this mission is by ensuring cases are distributed in the most effective and efficient way.

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

A: This is probably true for most supervisors, but employee relations is the most challenging portion of my job. I am dealing with people and their ability to make a living, so there are times when I have to make some very difficult decisions. Throughout my 20 odd years as a supervisor, I have developed strategies to work through these decisions, but it's never easy. I got into a supervisory role because I like to deal with people, especially the coaching portion, so I really try to focus on opportunities when I'm dealing with an employee relations issue.

Q: What would you like to share about the work that was done to achieve a stable state with the inventory?

A: I am exceptionally proud of the investigative workforce and the work put in over several years to improve production, while maintaining high-quality products. I have been particularly proud of our supervisors and everything they are doing to ensure efficiency and quality. From a metrics standpoint, I believe we are boasting under 2% of cases that are returned from the Quality Team for rework.

The field workforce has continued this incredible job through COVID operations. I have always been proud of our ability to be flexible and adapt, and this period of time has been no different. Our teams are getting the mission done and are doing it well.

JASEN SNYDER

Special Agent, Western Region

Q: What is a typical workday like as a special agent?

A: I'm an early bird, so I start around 5:30-6:30 a.m. I turn on my computer, answer emails, type and transmit cases, and prepare for the field work I have scheduled for that day. The field work includes subject interviews, source interviews, obtaining records, collaborations with colleagues, etc.

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

A: I immediately access the Personnel Vetting Processing System (PIPS) and scan the case messages, if there are any. I do that because I like to have a heads up on the case I will be working. I want to know ahead of time if there are foreign issues, financial issues, medical issues, criminal issues, etc.

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

A: There are so many different answers to this question. I have always been a stickler for quality. I also know how much these investigations cost, and I want the client to know that we conducted a thorough investigation, above reproach, so they won't have any reason to question if they are getting their money's worth.

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

A: Traffic, travel time. Out here in Los Angeles, it can take me an hour to travel 15 miles. It's getting worse, especially in the city.

Q: How do you prepare for an interview?

A: I've mentored a couple of agents, and the number one thing I tell new hires when preparing for an interview is to BRIEF, BRIEF, BRIEF. "Briefing" means to thoroughly review the Standard Form 86 (SF-86), all case messages, and make notes on apparent issues or any issues that you feel may arise during the interview. An example is when an applicant lists foreign travel to visit family/friends, yet there are no foreign contacts listed on the SF-86. I print out and go over case papers with a fine-tooth comb. Every agent has their own briefing method, you just have to figure out what works best for you. Once I brief the case, I'll have my folder with me with all of my blank releases just in case anything develops.

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

A: For me, the constant need to adapt to change is the most difficult, but it's something I know I have to do. There have been many occasions in which something that was scheduled, such as a source interview, needed to be rescheduled at the last minute due to situations beyond anyone's control. Or there are times when a source, or even a subject, doesn't show up for the interview. Adapting to the constant changes in policy/reporting can be tough as well, but again, I know it's a part of the job.

> *"I want the client to know that we conducted a thorough investigation, above reproach, so they won't have any reason to question if they are getting their money's worth.*

Q: Prior to COVID-19, how many cases are you assigned on average a week?

A: Cases are generally assigned based on the level of work you have completed. I'm typically working on 15 to 20 cases at a time.

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

A: I was given the opportunity to work abroad in Germany in the summer of 2018. I'm a member of the Training Advisory Group , and I've also participated in the Feds Feed Families program.

JOLYNN WEBSTER

Investigations Case Analyst, Quality Team

Q: What is a typical day like for an investigations case analyst?

A: My job as an investigations case analyst (ICA) is to ensure the completeness of each case by reviewing and evaluating investigative fieldwork against the Federal Investigative Standards (FIS) to confirm all guidelines have been adhered to and met. My first action in the morning is to order new cases, and I receive a daily case accountability list to work. I review each case in our case processing system in order to gain a "whole picture" of the applicant. This includes details such as when the case was scheduled and the results of the investigative work completed.

At the end of review, cases are either completed and sent for adjudication, reopened for missing items, scheduled for additional items, or sent to the Counterintelligence and Threat Coordination Activity (CITCA) for evaluation and potential referral to outside criminal and intelligence agencies for further action.

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

A: ICAs are the only entity who see the entire, completed case and provide the final review before it is sent to adjudication. It is our job to ensure that adjudicators have a complete investigation so they can render an appropriate clearance decision.

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

A: The majority of my day is spent reviewing the case to make sure investigative work is complete in accordance with national standards.

Q: Where do you see the BI mission going from here?

A: Since our transition from the Office of Personnel Management (OPM) to the Department of Defense (DoD), I like the progress being made. We recently made some great strides to deploy a fully electronic process for case review. I've been happy to see that grow and expand. I can't think of a better place to work, which is exactly why I came back to this mission after 18 years of being away from the workforce to raise my family.

> *"I can't think of a better place to work, which is exactly why I came back to this mission after 18 years of being away from the workforce to raise my family.*

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.

January's ACCESS will feature more firsthand accounts from DCSA's Personnel Vetting mission.

DoD CAF ACHIEVES HEALTHY INVENTORY AND TIMELINESS

By Kristine Racicot
Department of Defense
Consolidated Adjudications Facility

In May, the Department of Defense Consolidated Adjudications Facility (DoD CAF) reached a milestone two years in the making when the inventory of cases dropped below 80,000. At its peak in February 2019, the case inventory stood at 212,000. In addition to achieving a healthy inventory, DoD CAF met the adjudicative timeliness requirements of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA) for initial Secret (T3) and Top Secret (T5) cases.

"We are now able to maintain 60,000 to 80,000 cases in inventory, but that means little if we are unable meet the timeliness requirements outlined by IRPTA," said DoD CAF Executive Officer Jeffrey Robison. "IRPTA requires that the fastest 90% of initial T3 and T5 cases are adjudicated within a 20-day goal. A major milestone in achieving our healthy inventory was a record-setting performance in December 2019, when in less than two weeks the DoD CAF closed approximately 74,000 periodic reinvestigations. This unprecedented achievement was the 'spark' that ignited the adjudicative engine, propelling us to where we are today."

"During FY19, I set out to lead the DoD CAF in conquering the backlog of background investigations by establishing three strategic objectives: reduce inventory size, reduce inventory age, and enhance the quality and consistency of decision making and processes," said Acting Assistant Director Marianna Martineau. "These objectives are in line with the DoD CAF mission, which is to deliver informed and timely adjudicative decisions, supporting a trusted workforce to enable operational readiness and risk management."

First, to reduce inventory size, the DoD CAF applied a "portfolio approach" to inventory management. Adjudicative staff who previously performed non-adjudicative duties started adjudicating cases full time. The DoD CAF hired short-term contractors to reinforce their efforts, expanding over time.

Second, to reduce inventory age, the DoD CAF targeted case reductions through continued, detailed inventory management. Additionally, the DoD CAF adopted a mindset of handling "in-progress work" first, while enhancing e-Adjudication, in collaboration with the Performance Accountability Council (PAC) Program Management Office (PMO), security executive agent, and suitability executive agent.

Lastly, to enhance quality and consistency, the DoD CAF reorganized and leveraged the Lean Six Sigma method to improve efficiency of case assignment and upfront adjudicative business processes to eliminate steps that did not add value.

"By implementing these changes, we have been able to look into the future," said Martineau. "We look forward to exploring and introducing technological innovations, in coordination with the National Background Investigation Services (NBIS) Program Executive Office (PEO) and the Defense Information System for Security (DISS) PMO."

Continue reading below to learn more about "a day in the life of an adjudicator."

A DAY IN THE LIFE: ADJUDICATION

CANDACE WILLIAMS

Adjudicator, DoD CAF

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

A: On any given day, adjudicators review a variety of cases, including initial investigations, reinvestigations, continuous evaluation alerts, and incident reports. Depending on the security concerns present in the case, we may be able to make a favorable determination. If security concerns are not mitigated based on the information in the case, then we will likely draft some form of correspondence, whether it be a memo requesting more information from the command/subject or documents proposing denial or revocation of a subject's eligibility for access to classified information that explain the concerns supporting that decision.

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

A: When I get a new case, I look to see what kind of case I have, so I know what kind of information I will be reviewing, whether it be a Tier 3 (Secret) or Tier 5 (Top Secret) investigation, a Tier 3R/5R reinvestigation, or incident report documentation such as law enforcement reports. I also look to see what the subject's personnel category is (industry, military, or civilian), as that can affect how we communicate information to the subject and/or security officers. Then I dive in and read every page of documentation that has been provided.

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

A: Adjudicators have to be decisive and efficient critical thinkers to make quality adjudicative decisions and meet timeliness standards, ensuring mission readiness and risk mitigation. We require a strong knowledge of the policies and procedures that govern adjudications. We also need to be able to efficiently review a subject's case, identify the information relevant to national security, and be able to discern whether the subject, all-things-considered, poses an unacceptable security risk.

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

A: Drafting correspondence, whether to request more information or to recommend denial/revocation of a subject's eligibility, takes up the majority of my day. It's one of our most time-consuming tasks. However, it also means you probably have an interesting case with important security concerns that need to be addressed.

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

A: We are continuously learning new policies and procedures that govern adjudications. The landscape of national security is ever-changing, so being able to change the way you work to meet mission needs over time is essential, and that can be challenging at times.

> *Adjudicators are a diverse group of professionals. We are former teachers, military service members, investigators, psychologists, and have many other experiences that can provide unique and valuable perspectives.*

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

A: Adjudicators are a diverse group of professionals. We are former teachers, military service members, investigators, psychologists, and have many other experiences that can provide unique and valuable perspectives.

LEBONA HAILU

Adjudicator, DoD CAF

Q: What is a typical day like for you?

A: The first thing I do when logging in each morning is load up all of the different applications and websites that allow me to effectively complete my work for the day, including the Defense Information System for Security System (DISS) and the Joint Personnel Adjudication System (JPAS). After that, it's just case by case for the rest of the day. That is not to say my day is mundane. Every case is different, and every case brings a new challenge with a variety of actions.

> *Adjudicators truly protect the integrity of the U.S. government's workforce.*

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

A: When receiving a new case, I make sure that I have the most up to date investigations and information for the subject of the case, which sometimes requires me to do a little digging into DISS and JPAS. These databases are really important for adjudicators and help us make the best clearance eligibility determinations. Without the information required to adjudicate the case, we cannot proceed, which is why the first step is critical. It's like taking inventory so you know what you have, what you don't, and what you need to request.

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 role as an adjudicator is quite literally the gatekeeping portion of the DCSA mission. Adjudicators truly protect the integrity of the U.S. government's workforce. We strive to ensure that the individuals who are granted security eligibilities are those who are able and willing to safeguard classified national security information or occupy sensitive positions without any threats or vulnerabilities that could cause them to do otherwise.

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

A: The majority of my day is spent reading through investigations. Sometimes they can be 70 pages or 700 pages, but that is always where we find the most valuable and relevant information for the adjudication process. Additionally, I spend my time analyzing any issues found in the investigation and using the "whole person concept" and other evidence to determine whether the issues are disqualifying or can be mitigated.

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

A: The most challenging part of my job is assessing risk factors for individuals from different backgrounds. Every case is different, and each carries varying levels of risk, so being able to accurately assess that requires patience and practice.

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

A: Probably that my job exists! I don't think the majority of the American public knows anything about adjudications or how the process it works — it is a relatively well-kept secret. The only people who seem to know about it are government employees, contractors, military personnel, and their families. But I will say that a more specific fact about my position is that adjudicators do not allow subjective emotions to affect their adjudication determinations. It is virtually impossible for me to make a clearance determination based on my own opinions or perspectives. Every decision must be backed by supporting evidence, and I think that is extremely important and noteworthy.

MICHAEL RUPP

Adjudicator, DoD CAF

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

A: I cannot speak for all adjudicators but for me there is no "typical" day. Every day presents new challenges. As a DoD CAF adjudicator, I grant, deny, and revoke eligibility for Homeland Security Presidential Directive 12 (HSPD-12), suitability, child care, national security, and industry programs. My adjudications cover military, civilians, and contractors. I work a wide variety of cases, from new investigations to continuous evaluations, incident reports, public trust, and child care cases. I often think to myself (in my best Forrest Gump impersonation), "Cases are like a box of chocolates, you never know what you are going to get."

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

A: The first thing I do is review the Case Closing Transmittal (CCT) and the Agency Use Block (AUB) contained in the investigation. The CCT provides a summary of investigated activities and results, and the AUB provides extra coverage codes, sensitivity level/risk, access/level, position codes, and special handling information. Next, I screen the Defense Information System for Security (DISS) for case notes or customer service requests. I don't want to spend time working a case I can't make a decision on because some cases require special teams to work them.

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 making sound and timely decisions concerning individuals that are in the best interest of national security and allow that individual access to accomplish the mission.

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

A: Reading, reading, then there is a lot of reading followed by more reading. The investigations that I receive can average from 30 to 500 or more pages. I would have to say reading takes up the majority of my day.

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

A: Keeping up with change. Of all the jobs I have had in 30-plus years of working, this has been by far the most challenging. There are policies, guidelines, and procedures for every type of investigation. On a daily basis, I apply four different sets of adjudicative guidelines across various case types and programs. Guidelines are established as the single common criteria for all U.S. government civilian and military personnel, consultants, contractors, licensees, certificate holders or grantees and their employees, and other individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. There are guidelines for security, suitability, HSPD-12 and child care. Successfully adapting to change is challenging for any job, but in my experience, this job has been the most challenging. No two cases are the same.

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

A: As an adjudicator, not only do I directly affect national security, I also affect the lives of thousands of people every year. Because of that, I take my job very seriously.

January's ACCESS will feature more firsthand accounts from DCSA's Personnel Vetting mission.

DCSA'S COUNTERINTELLIGENCE MISSION

DCSA's Counterintelligence mission is the federal government's strongest link between the nation's industrial base, the U.S. Counterintelligence (CI) and Intelligence Community (IC), and federal law enforcement. No other agency has the level of contact with industry — our partners on the ground who see and report adversary threats firsthand. Other agencies in the IC focus on singular threats, while DCSA can see the whole picture of threat across the entire industry. This collaboration ensures effective communication and information sharing to identify threats to cleared U.S. personnel and our nation's critical technologies as well as articulate those threats back to industry and U.S. government leadership.

COUNTERINTELLIGENCE BY THE NUMBERS

Produces on Average **5,629** Intelligence Information Reports

Processes over **46,565** Raw Reports from Industry

Develops over **7,702** Suspicious Contact Reports

CUTTING THROUGH THE FOG: RAISING COUNTERINTELLIGENCE AWARENESS IN THE AGE OF SOCIAL DISTANCING

By Raleigh Wilson
Cypress Field Office

The spread of COVID-19 was like a sour fog, silently seeping into corners across the nation, upending commonly held norms and practices. Those working towards national security goals were equally affected. DCSA directed counterintelligence special agents (CISA) to work from home under "maximum telework," and CISAs faced a paradoxical set of questions such as: how does one dutifully execute the counterintelligence (CI) mission while working from home? How will our adversaries exploit societal disruption to target sensitive programs within the Defense Industrial Base (DIB)? And how can DCSA CISAs continue their work of raising CI awareness within the DIB while being sensitive to collective anxiety, sickness, and death?

Immediately following the start of maximum telework, CISAs in the Western Region began work on myriad solutions to provide effective and timely CI education and outreach to cleared contractors. Due to recent personnel changes, many newly assigned CISAs also had to innovative methods to establish strong relationships with key cleared personnel. Such an interpersonal undertaking, with its individual nuances, was a daunting challenge at best, but necessary during a pandemic. The CISAs thoughtfully considered the situation, "red teaming" how adversaries could take advantage of COVID-19 precautions to target the DIB and developing corresponding CI awareness and education mitigations. They also assessed how to best leverage available resources to broadcast their message while building personal relationships in an unclassified, virtual operating environment.

CISAs recognized that many cleared contractors were implementing a blend of maximum telework for high-risk and telework-capable staff, including many facility security officers (FSO). Additionally, massive layoffs and work-hour reductions plagued the nation, which potentially affected the household incomes of many cleared contractor employees. CISAs developed a working theory that adversaries could leverage possible financial difficulties and exploit social distancing to target cleared contractors. To raise awareness of such eventualities, CISAs leveraged unclassified, open source case study information to develop a short CI awareness note and call to action for FSOs. The FSOs, in turn, could provide the information to their respective cleared employees.

Despite COVID-19 social distancing restrictions, cleared contractors expressed an appetite for CI engagements and awareness briefings. However, CISAs were in no position to do what they loved to do — visit facilities, learn what cleared contractors do, and provide focused CI awareness briefings to harden contractors against adversary targeting. A few weeks before moving to maximum telework, CISAs received a briefing from DCSA headquarters about the Adobe Connect platform and leveraging the platform to provide virtual briefings. Next CISAs acquired Adobe Connect accounts and received comprehensive IT training to familiarize themselves with the platform. Eventually, with some repetition and good luck, the CISAs were ready to provide briefings to cleared contractors.

Except it wasn't that easy. While CISAs are highly competent CI professionals, most are not familiar with the nuanced considerations pertaining to information systems and applications within the DoD enterprise. CISAs started testing Adobe Connect at a small scale to identify potential snags and long-term platform viability. They learned that, given their equipment at the time, projecting audio through the system would likely be difficult. The hunt for an audio solution began shortly thereafter. The CISAs collaborated with their DCSA colleagues to obtain dedicated teleconference lines, guaranteeing robust audio support to virtual presentations, and understand information system classification considerations. They subsequently leveraged open sources and the Center for Development of Security Excellence (CDSE) to develop unclassified CI awareness briefings to pair with the Adobe Connect system. Finally, CISAs produced multiple field guides and papers outlining their process to enable others to leverage the same capabilities.

CISAs also developed a subsequent initiative to address an emerging mission gap: providing comprehensive CI support to the Personnel Vetting mission. The formal creation of DCSA in October 2019 provided new opportunities to integrate CI with security functions, including personnel vetting for security clearances. CISAs developed an elemental CI training program to assist background investigators in identifying CI threats during the course of their standard operations. Background investigators found value in the training and expressed interest in expanding the program. Integrating the video teleconferencing platform with the personnel vetting CI training program set conditions for strategic program growth.

Even within the pandemic environment, CISAs were able to use their newfound capabilities to counter threats to critical programs and drive greater security across the DIB. One of the products developed to support CI awareness enabled a resolute FSO to raise CI awareness among cleared employees, resulting in a 600% increase in suspicious contact reporting. Another contractor promptly reported a suspected insider threat, and CISAs leveraged their resources to actively coordinate with national security partners to mitigate the threat to critical defense programs. Shortly after receiving CI training, personnel security investigators identified ten incidents of potential CI concern. CISAs subsequently determined eight of the incidents were validated threats and collaborated with national security partners to proactively mitigate threats to sensitive national defense information.

Adversaries will continue to target sensitive programs and critical employees within the DIB and will adjust their tactics to navigate the pandemic response. DCSA and its partners will be there to meet them.

A DAY IN THE LIFE: COUNTERINTELLIGENCE

WESLEY "WES" R. STEWART

Counterespionage Branch Chief, Counterintelligence Operations Division

Q: What is a typical day like for you?

A: There is no such thing as a typical day within Counterintelligence (CI) headquarters. Most days consist of many meetings, teleconferences, and project coordination. I generally check in with my team to address any support they may need executing their assigned projects and then it's off to the races. I am heavily engaged in DCSA's organizational development activities as we merge our missions and establish the necessary policies and standard operating procedures. This requires a substantial amount of coordination across the enterprise as we build the agency's defensive CI capability to protect against foreign intelligence threats to DCSA's personnel, information, operations, and property.

> *"Running a counterespionage program is a constant exercise in intellectual humility. One must be continuously learning and seeking insights from those around you to be successful in this position.*

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 creating and facilitating an environment wherein our CI enterprise can adequately and efficiently protect DCSA from foreign intelligence entities and help ensure the agency's fundamental mission areas can operate without interference. The aspect of my job that takes up the majority of my time is articulating CI policies and educating our internal workforce, external partners, and senior decision makers on the appropriate conduct of authorized CI activities.

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

A: The most challenging part of my job is building the necessary coalitions among mission partners and decision makers to identify CI threat information and coordinate it appropriately, while actively participating in an ongoing merger of a new defense agency. This is also one of the most satisfying aspects of my job.

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

A: Running a counterespionage program is a constant exercise in intellectual humility. One must be continuously learning and seeking insights from those around you to be successful in this position. Counterespionage is not a one-way street.

JOHN "JAY" KEARNEY JR.

Cyber Counterintelligence Liaison Officer, National Cyber Investigative Joint Task Force

Q: What is a typical day like for you?

A: A typical day for me consists of many meetings and answering requests for information (RFIs) from the 35 partner agencies in the FBI's National Cyber Investigative Joint Task Force (NCIJTF), as well as DCSA Counterintelligence divisions like Cyber, Operations, and Analysis. I review internal NCIJTF reporting and provide relevant DCSA information. I also reach out to field elements in order to bridge the relationship between DCSA and the law enforcement (LE)/ counterintelligence (CI) community.

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

A: The most important part of my job is to be a conduit of information, not just to DCSA, but to NCIJTF and the LE/CI community. DCSA is a smaller agency compared to some of the NCIJTF partners, and so being able to provide solid data to enable action on our adversaries is critical and a great position to be in.

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

A: Coordinating, integrating, and sharing information takes a bulk of my time. But at the same time, I also need to wait on the LE/CI community to take action or respond to DCSA's requests. When we are limited in our authorities and rely on other government agencies to take action, it's a tough spot to be in at times.

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

A: The most challenging aspect of being a liaison officer (LNO) is the feeling of having to be everything to everybody. I think internal to DCSA, everyone has their own roles and responsibilities. But being detailed to another government agency, the expectation is that you are a "one stop shop" for your home agency. Whether it's CI, industrial security, or personnel vetting, you need to have solid contacts within DCSA in order to reach out and provide good information. That said, I look forward to the challenge.

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

A: Some may not know this, but as LNO to NCIJTF, I've gotten to meet and shake hands with former United Kingdom Prime Minister David Cameron as well as recent FBI Directors Robert Mueller, James Comey, and Christopher Wray. Those interactions took place at tours or briefings at the NCIJTF, where I was able give a quick intro and explain DSS/DCSA. We have LNOs in Australia, New Zealand, and the U.K., and I've gotten to meet each of those ambassadors at LNO turnover events. It's a great perk to have such unique opportunities with the NCIJTF partners and our Five Eyes (FVEY) intelligence alliance with Australia, Canada, New Zealand, the U.K., and the United States.

ERIC E. WALLACE

Counterintelligence Special Agent, Southern Region

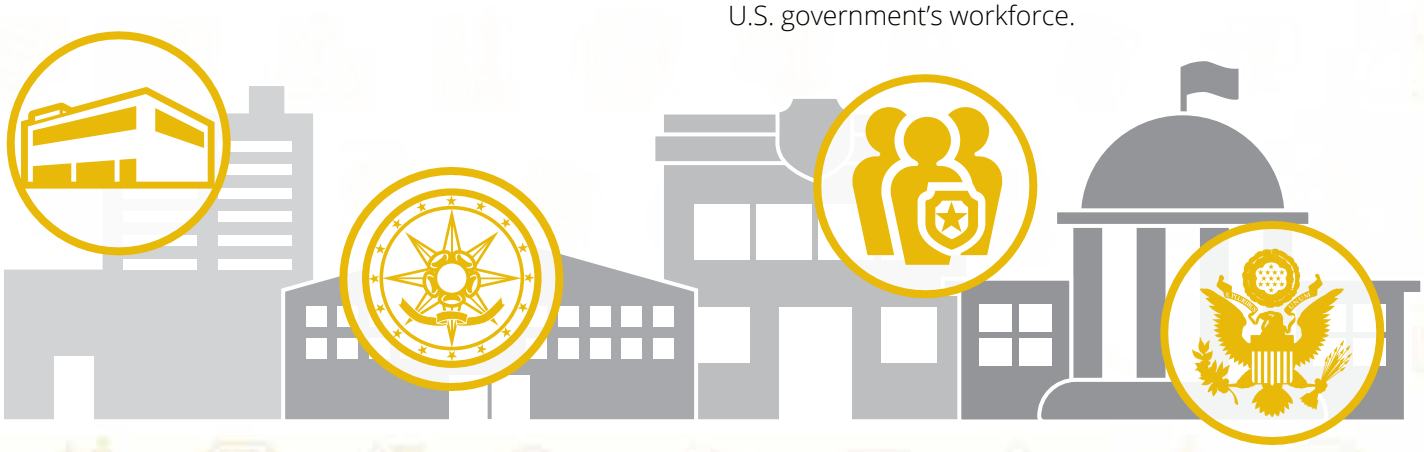
Q: What is a typical day like for you?

A: A typical day for me consists of talking with people and reviewing and documenting incoming suspicious contact reporting from cleared contractors. I really enjoy all the people I meet and interact with in my job. I have the opportunity to speak with DCSA team members from every directorate in the agency. I regularly coordinate my efforts with the industrial security representatives (ISRs) and information system security professionals (ISSPs) in the Huntsville Field Office. I discuss insider threat issues with background investigators in Huntsville and personnel vetting issues at headquarters.

I work closely with DCSA cyber and analysis personnel to pass information and receive assistance when I need help. I also routinely coordinate and share information with the military components' counterintelligence offices, the Federal Bureau of Investigations (FBI), and numerous other government agencies. I speak with facility security officers (FSOs), key management personnel, information technology personnel, engineers, scientists, human resources, and many other employees at our supported cleared contractor sites. It seems like I get to interact with someone new and interesting every day.

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

A: I am fortunate in that my job allows me to touch all aspects of the DCSA mission. Foreign intelligence entities work to compromise the trustworthiness of the U.S. government's workforce, the integrity of its cleared contractor support, its technologies, services, and supply chains. So, I work to detect and deter those entities' efforts targeting cleared contractors and the U.S. government's workforce.



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

A: The majority of my day is taken up by talking with people to detect foreign intelligence activity and to deter that activity from taking place. The most challenging aspect of my job is explaining counterintelligence. For the uninitiated, counterintelligence can seem to be part science, part wizardry, part luck, and part fiction. In truth, it is some of it all.

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

A: I think one large misconception about counterintelligence is that we focus primarily on what foreign governments want to steal and how they would steal it. Our concern with cleared industry is in stopping and identifying those foreign government attempts.

RALEIGH D. WILSON

Counterintelligence Special Agent, Western Region

Q: What is a typical day like for you?

A: There is no "typical day" for a Counterintelligence (CI) professional. On any given day, one could be out of the office providing CI awareness briefings to industry, meeting with industry leaders and experts, or collaborating with U.S. Intelligence Community (IC) and law enforcement (LE) partners. One could also spend an entire day in the office drafting reports, reviewing suspicious reports from industry, and collaborating with other DCSA directorates. Usually, a day's work is a combination of all of these activities sprinkled with ad hoc surprises.

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

A: There is really a two-fold process that is central to my job: expertly advising and educating industry on CI threats so they know what to report and fusing industry-derived threat information with the IC and LE partners. Within the CI community, counterintelligence special agents (CISAs) have unique access to cleared industry and are at the forefront of identifying threats to critical technologies and cleared personnel. Through various reporting channels, we fuse that threat information with our interagency partners, enabling them to take action to mitigate the threats. Additionally, we use the threat information to fill critical IC intelligence gaps pertaining to strategic threat trends.

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

A: Coordination and documentation are constant, time consuming, and necessary. CI is a dynamic discipline. Bad actors, interagency partners, and cleared contractors are constantly changing, operationally moving, and reacting to one another. The confluence of activity creates an ever-shifting landscape. Constant coordination and communication between fellow CISAs and our interagency partners are absolutely crucial to overcome challenges associated with that environment. As such, drafting and publishing, especially clear and detailed reports, is central to our mission. Time spent publishing and coordinating reports with our partners is disproportionally larger than time spent acquiring threat information.

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

A: The CI discipline is not well understood and is more art than science. This is a challenge, given CI professionals rely almost exclusively on others to assist them in identifying threats. CI professionals must constantly help those around them understand the CI perspective of a given situation to achieve mutual goals.

> *"We don't typically resolve issues in an hour or have a big, magic screen that tells us every detail about bad guys as depicted in TV shows and movies.*

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

A: We don't typically resolve issues in an hour or have a big, magic screen that tells us every detail about bad guys as depicted in TV shows and movies. We wish we had those all-knowing systems at our fingertips! In reality, that type of detail takes a significant amount of work by a large team of agents, analysts, and support professionals.

January's ACCESS will feature more firsthand accounts from DCSA's Counterintelligence mission.

THE NATIONAL SECURITY LEARNING CENTER

The National Security Learning Center (NSLC) is DCSA's security center of excellence, created to professionalize the security community and provide security education, training, and certification for the Department of Defense (DoD) and industry.

THREE INSTITUTIONS

NSLC's three educational institutions provide development, delivery, and exchange of security knowledge to ensure a high-performing workforce. The NSLC supports the DCSA workforce, DoD, and industry in their efforts to address our nation's security challenges.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

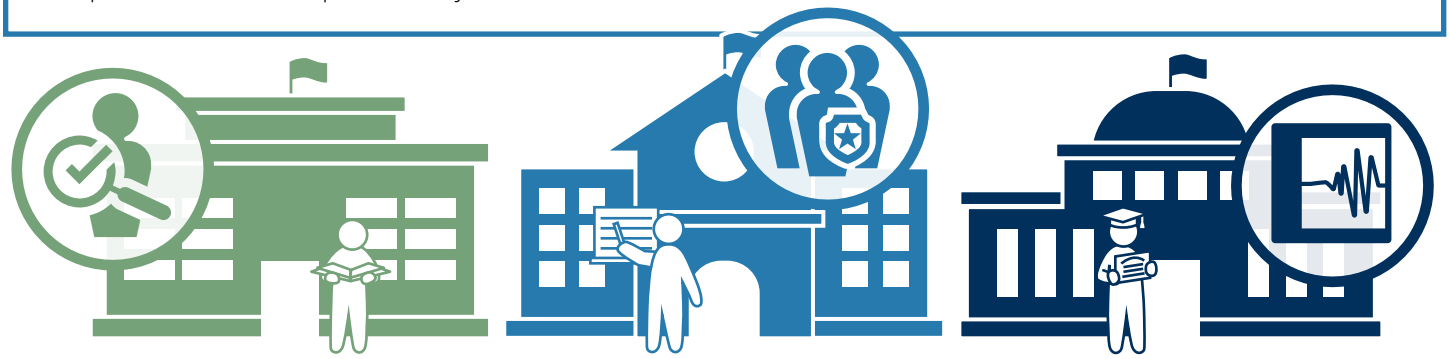
Established in 2010, the Center for Development of Security Excellence (CDSE) offers security and awareness products and services to civilian and military personnel within DoD, employees across the federal government, and cleared contractors under the National Industrial Security Program (NISP). Security professionals make use of resources such as job aids, webinars, security awareness games, and training videos to gain training, education, and certifications throughout the entirety of their professional development lifecycle.

1.68M Course Completions

7 Certifications & **1** Credential
(6 Certifications with National-level Accreditation)

ACE **33** Courses with American Council on Education (ACE) Credit Recommendations

Over **591,000** Toolkit Visits



NATIONAL TRAINING CENTER

The National Training Center (NTC) provides training programs for DCSA background investigators, quality reviewers, and suitability adjudicators. A Federal Law Enforcement Training Accreditation (FLETA)-accredited academy, NTC provides a variety of courses to DCSA partners on background investigations systems and processes. Onsite training is available as well as formal recurring training in the field including two accredited training programs.

6 **FEDERAL BACKGROUND INVESTIGATION TRAINING PROGRAM:** A 6-credit, 5-week program designed for new special agents.

3 **INVESTIGATIONS CASE ANALYST PROGRAM**: A 3-credit, 23-week program designed for new investigations cases analysts and security assistants.

NATIONAL CENTER FOR CREDIBILITY ASSESSMENT

The National Center for Credibility Assessment (NCCA) conducts credibility assessment, training and education, research and development, technical support, and oversight activities for federal polygraph and credibility assessment mission partners. Established in 1951 as the U.S. Army Polygraph School, NCCA is responsible for the development and implementation of polygraph training, the continuing education and certification of polygraph examiners, inspection oversight for all federal polygraph programs, and advancing any new research, techniques, or technologies related to credibility assessment. Beginning October 1, 2020, operational control of NCCA transferred from Defense Intelligence Agency (DIA) to DCSA.

CDSE LAUNCHES INSIDER THREAT SENTRY MOBILE APP TO PROMOTE AWARENESS, VIGILANCE

By Amber Yi
Center for Development of Security Excellence

In June, the Center for Development of Security Excellence (CDSE), an educational institution of the National Security Learning Center (NSLC), successfully launched its first mobile app: the Insider Threat Sentry. Available for both iOS and Android devices, the app expands the availability of posters, videos, security awareness games, job aids, case studies, and other materials.

"These days everyone is on their mobile device," said Rebecca Morgan, chief of CDSE's Insider Threat division. "The app gives us another way for people to access insider threat awareness content. We're thrilled that it's been so well received and that people are engaging with it."

One of the app's key features is exclusive materials, including posters, graphics, and bite-sized pieces of information. During the app's 18-month research and approval phase, CDSE fielded extensive feedback on the types and frequency of content preferred by users. "One of the things we heard most often was that people wanted new, exclusive content, and we're using Sentry to provide that," Morgan said. "We aim to push out something new at least once a month so we can continue to deliver on that request."

The Insider Threat Sentry app also aims to connect users with conferences, webinars, symposia, and awareness campaign, such as September's National Insider Threat Awareness Month. This annual event, coordinated among CDSE, the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), the National Insider Threat Task Force (NITTF), and the National Counterintelligence and Security Center (NCSC), features a variety of events and counter-insider threat activities.

This multi-agency partnership is ongoing. OUSD(I&S) and NITTF partnered with CDSE on the creation of the Insider Threat Sentry app, as its features and purpose align with their respective office missions and goals.

Dr. Brad Millick, director of DoD's Counter-Insider Threat mission at OUSD(I&S), stressed the importance of raising awareness as the impetus behind the app. "Awareness of insider threat helps our programs deter, detect, and mitigate risks associated with trusted insiders," he said. "The information in Sentry facilitates early intervention opportunities for our programs, strengthens our nation's resiliency, and fosters rehabilitative outcomes for personnel at risk."

"Awareness and vigilance are not about curtailing protected free speech or legitimate government whistleblowing," said Morgan. "They're about preventing the exploitation of authorized access to cause harm to an organization or its resources. The best way to prevent that from happening is ensuring that the workforce is engaged and aware."

NITTF Director Charles Margiotta agreed that proper training and tools to detect anomalous behavior, along with early intervention, are the most critical element of insider threat programs. "Many institutions have perimeter defenses, such as gates, guards, access controls, and computer firewalls, but they are still vulnerable to the insider threat," he said. "By increasing engagement and awareness with tools like Insider Threat Sentry app, we can reduce acts of harm to self or others, prevent the loss or compromise of classified information, and minimize damage to organizations."

NSLC Director Kevin Jones noted that increasing mindfulness of potential insider threats is an ongoing effort. "Insider threat awareness training is not a one-time event, and it does not need to occur in a classroom," he said. "Learning is a process and we provide resources to facilitate long-term engagement with the workforce. CDSE is a 'space,' not a 'place.' With the Insider Threat Sentry app, we are providing anytime, anywhere access to that space and the tools to remain vigilant about national security risks."

Insider Threat Sentry is free to download in the respective app stores for iOS and Android devices within the United States.

A DAY IN THE LIFE:
NATIONAL SECURITY LEARNING CENTER

DANNY JENNINGS

Branch Chief for Security Training, Center for Development of Security Excellence

Q: What is a typical day like for you?

A: As a first-line supervisor, what takes up the most of my day is managing resources and manpower programs, project meetings for team development on training, and ensuring the new online training is effective during the COVID-19 environment. My job runs the whole gamut of tasks and responsibilities. You are a supervisor with all of the administrative duties of a supervisor. You have to understand the intricacies of the many projects that each section is involved in to make informed decisions on the team's goals and directions.

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

A: To ensure that we are providing the best training, we will follow our internal processes to analyze the request and determine if training is a solution to the problem. If we believe there is a training product that needs to be developed, then it goes through our process of design, development, implementation, and evaluations for the best possible solution. If it is not a problem that training can solve, we provide courses of action for consideration.

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 the transfer of knowledge to a national security workforce to better prepare it to counter threats and protect critical assets, whether through an eLearning course, how-to job aid, or resurrecting a virtual instructor-led course during this COVID-19 pandemic. We appreciated the director's comments recently that our training is an extremely important mission set for national security.

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

A: Meetings, meetings, and more meetings, and collaboration on executing training objectives.

Q: How do you prepare for being a branch chief?

A: I've been very fortunate to come up through the ranks, touching each security focus area (Counterintelligence, General Security, Industrial Security, Information Security, Insider Threat, Operations Security, Personnel Security, Physical Security, and Special Access Programs), so my experience has provided me with subject matter expertise in my current role. However, managing and understanding culture, business processes, and leading people is also a primary focus.

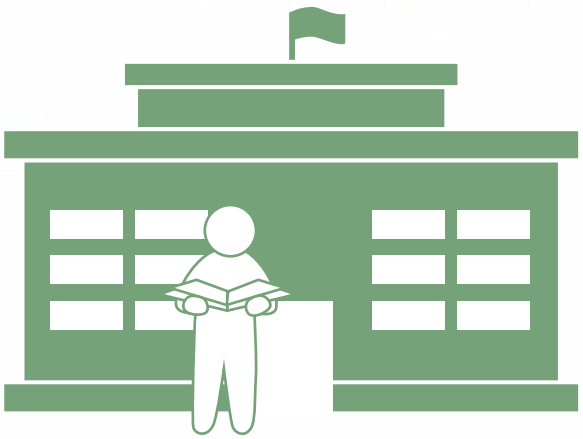
> *"The most important aspect of my job is the transfer of knowledge to a national security workforce to better prepare it to counter threats and protect critical assets*

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

A: The most challenging aspect of my job is balancing competing priorities against limited resources, and managing the environment and expectations of upper-level management, stakeholders, and employees.

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

A: In my role, you need to be flexible and invest in people. Behind every tasking, there is a person. If we take care of our people, the work will take care of itself.



VICTORIA BARTH

Supervisory Instructional Systems Specialist, Center for Development of Security Excellence

Q: What is a typical day like for you?

A: Every day is different and presents new challenges — that's what makes it fun and exciting. Take COVID-19 as an example. No one could have predicted this pandemic and the impact on our daily lives, but because of social distancing requirements, we've had to find innovative ways to deliver essential training content to the workforce. Teamwork is what has allowed us to meet these challenges head-on every day. For example, the collaborative work environment enabled us to rise to the challenge of converting some traditional instructor-led courses to a virtual environment. Such a heavy lift would not have been possible without teamwork.

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

A: The first step when we receive a new training request is to do an analysis of the problem we are trying to solve, the target audience, the constraints and drivers, the timeline, and the availability of resources. Once these questions are addressed, we can propose several solutions, with the pros and cons of each relayed to the stakeholders. Ultimately, the goal is to ensure that the proposed training solutions remediate whatever gap exists. Often, more than one product may be required to completely address the need, possibly necessitating a phased implementation approach. So, whether it is a webinar, eLearning course, job aid, performance support tool, or a multi-faceted solution, the team will work to ensure that the needs of the workforce are met in the most efficient and effective way possible.

> *Every day is different and presents new challenges — that's what makes it fun and exciting.*

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 to ensure security professionals receive the training they need to effectively do their jobs and safeguard the nation. Additionally, delivering awareness training for non-security professionals is also essential for national security. Ensuring the design, development, delivery, and maintenance of all learning products for these groups is the main focus of my duties.

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

A: The majority of my day is spent collaborating with my team, consulting stakeholders, working with subject matter experts, and partnering with members of other workgroups to ensure training objectives are met. Nothing can be done in a silo, so teamwork and communication are key to effectively executing projects in a timely manner.

Q: How do you prepare to be an Instructional Systems Specialist?

A: There are different routes people can take to become an instructional systems designer (ISD) or specialist. Some people go through formal education, others take certificate programs, while still others transition from alternative learning fields. No matter how someone gains the requisite pedagogical knowledge, real-world experience, coupled with mentoring from seasoned ISDs, is key to enabling someone to become an exceptional designer.

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

A: The most challenging aspect of my job is trying to manage competing priorities effectively. Everyone is being asked to do more with less. Resources are often scarce and stretched to the limit. Finding a way to meet all expectations while keeping team morale high can be a delicate act. As with most things, the key to striking the right balance is communication, not just among teams, but with stakeholders and senior leadership. By working together, we can achieve meaningful prioritization, thus enabling the best use of resources at any given time.

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

A: Something others might not know is that I used to be a teacher. Having that experience is not required of an instructional systems specialist, but it does help me see things from multiple perspectives. When I evaluate a product, I look at it not just as a designer, or even an end-user, but also as an instructor. Things often look good on paper, but they can fall flat in reality. My experience often allows me to see these potential pitfalls and head them off before time is wasted on products that ultimately will not meet the needs of the learner.

MARY STECH

Certification Security Specialist, Center for Development of Security Excellence

Q: What is a typical day like for you?

A: A typical day for me is managing five out of the seven certifications. I manage the Security Asset Protection Professional Certification (SAPPC), Security Program Integration Professional Certification (SPIPC), Special Program Security Certification (SPSC), Industrial Security Oversight Certification (ISOC), and Adjudicator Professional Certification (APC). In each program, I collaborate with the technical managers on the training within each program. I am a member of the governance board, which meets quarterly to ensure that the programs are running smoothly.

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

A: When we get a new certification, the first thing we do is wait for the policy and procedures to be put in place. Next are the blueprints and credentials, so that we can start building the certification. After the governance board approves it, we inform the stakeholders that the certificate policy was passed. Then, we work with the technical agencies and the subject matter experts to build the assessments and skill standards for that particular certification. Communication with everyone is key when implementing a new certification.

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 collaborating with the stakeholders and customers to ensure that the program and my job protect our mission and protect the nation's assets.

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

A: The majority of my day is devoted to the Adjudicative Security Program and collaborating with the stakeholders of each program I manage to ensure their needs are met.

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

A: The most challenging aspect of my job is delegating to new personnel within the virtual COVID-19 environment. It's difficult to ensure these onboarding personnel within my department are getting the proper information and training needed to do the job. Another challenge is finding ways for employees to connect with each other as a team while in a teleworking environment.

KIMBERLY "CRICKET" SMITH

Field Investigative Training Specialist, National Training Center (NTC)

Q: What is a typical day like for you?

A: Before the current COVID-19 conditions, we spent a great deal of time traveling to field office locations to train our background investigation field agents. When we're not conducting in-person or online training, we're making sure we have proficient knowledge of new and current policies and procedures so that we can help our field agents apply them to their day-to-day work. This includes creating new course materials for training courses that are in the design phase, making modifications to current courses following results of evaluations, liaising with other groups, helping improve course materials, expanding our knowledge base with professional development courses, and answering questions field agents may have about current policies and procedures.

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

A: As a field investigative training specialist (FITS), we use a "systems approach" to training development known as the ADDIE Model — Analysis, Design, Development, Implementation, and Evaluation. This approach begins with an analysis to determine what an individual must know to be able to accomplish the task being taught. Once the analysis is complete, we move to the design phase, in which we create learning objectives and the evaluation goals. In the development phase, we make lesson plans, learning resources, and course materials. From there, we move to the implementation phase, and we conduct a pilot test of the course. After the pilot test is completed and evaluated, we make any modifications necessary and the course is delivered. Finally, a series of evaluations are conducted. Based on information from the implementation and evaluation phases, we make final revisions before the course is delivered again.

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 the FITS position is helping to keep background investigators' skillset sharp so that they are able to obtain the best and most reliable information on their subjects. This investigation information is provided to the adjudicator, who then makes the determination whether the subject should be given (or maintain) a clearance to access sensitive and/or classified information.

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

A: My day can vary from day to day. Currently, the majority of my day is spent designing a new course for new agent coaches. I am also working with coaches overseeing new agents in our investigator field course. It is an eight-week long course, following a new agent's successful completion of the Federal Background Investigator Training Program (FBITP). On any given day, I also attend meetings with other members of the field investigation training team (FITT) to develop and maintain course materials. Everything the team creates is a collaborative effort.

Q: How do you prepare to be a Field Investigative Trainer?

A: Our team is made up of trainers from different backgrounds within the background investigations and national security fields. My personal background consists of a master's degree in criminology, followed by three years in law enforcement, from which I transitioned into a field agent position. As a field agent, I tried to diversify my career by volunteering for work outside of my normal duties across the agency. These volunteer opportunities included working with the training department as a class counselor for our new agent training program at our National Training Center, coaching new hires, shadowing, filling in for my special agent-in-charge, completing overseas missions with our International Group, and temporary assignments with our Integrity Assurance Group.

As a field agent, I tried to diversify my career by volunteering for work outside of my normal duties across the agency.

I found that my passion was in training. So, I continued to work on growing my knowledge and experience in that arena and was fortunate to come on as a field investigative trainer in April 2017. Additionally, upon joining the FITT, I completed the Law Enforcement Instructor Training Program (LEITP). This program is required by the Federal Law Enforcement Training Accreditation (FLETA) and is designed to provide training in law enforcement instructional skills, focused on curriculum development and delivery.

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

A: The most challenging part of the job for me is keeping up with policy and procedural changes and ensuring that those changes are made to all of our course materials in a timely manner for the field agents.

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

A: I think the field investigative training specialist title might make others think that we only train and instruct courses, but in actuality, we create and deliver our course materials. We see the process through from start to finish using the ADDIE model.

January's ACCESS will feature more firsthand accounts from DCSA's National Security Learning Center

DCSA RECOGNIZES THE BEST IN INDUSTRIAL SECURITY:

60 FACILITIES RECEIVE COGSWELL AWARDS IN 2020

On July 30, DCSA announced the winners of the annual James S. Cogswell Award for Outstanding Industrial Security Achievement, awarding 60 cleared contractor facilities the distinction. Traditionally, the awards are usually presented at the annual NCMS — Society of Industrial Security Professionals — training seminar. However, due to the COVID-19 pandemic, the seminar was cancelled, and the award winners were recognized in a virtual ceremony hosted by DCSA Director William K. Lietzau. The Cogswell Award winners represent the "best of the best," and the winning facilities' security programs stand as models for others to emulate. These 60 facilities represent less than one-tenth of 1% of the approximately 12,500 cleared facilities in the National Industrial Security Program (NISP).

The Cogswell Award was established in 1966 in honor of the late Air Force Col. James S. Cogswell, who articulated the underlying principle of the industrial security program: the need for a true partnership between industry and government to ensure the protection of classified information, materials, and programs.

Once nominated, facilities enter an eight-month internal review process by the national review team of DCSA regional directors and representatives from across the agency. The review team vets all nominations with 57 external agencies and makes recommendations to DCSA senior leadership for a final decision based upon the following criteria:

OVERALL SECURITY PROGRAM

SENIOR MANAGEMENT SUPPORT

SECURITY VULNERABILITY ASSESSMENTS

SECURITY EDUCATION AND AWARENESS

FACILITY SECURITY OFFICER (FSO) AND SECURITY STAFF LEVEL OF EXPERIENCE

CLASSIFIED MATERIAL CONTROLS

CONGRATULATIONS TO THE 2020 COGSWELL AWARD WINNERS!

Acuity, Inc.
Reston, VA

Advanced Acoustic Concepts LLC , A DRS/ Thales Company
Columbia, MD

AMERGINT Technologies, Inc.
Colorado Springs, CO

American Systems Corporation
Albuquerque, NM

Aquila Technology
Burlington, MA

ASM Research
Fairfax, VA

BAE Systems, Electronic Systems
Greenlawn, NY

BAE Systems, Electronic Systems
Wayne, NJ

BAE Systems, Electronic Systems
Nashua, NH

BAE Systems Land & Armaments LP
Arlington, VA

BAE Systems Land & Armaments LP
San Jose, CA

BAE Systems, Technology Solutions & Services, Inc.
California, MD

Crane Electronics, Inc.
Fort Walton Beach, FL

CyberPoint International, LLC
Baltimore, MD

Delphinus Engineering, Inc.
Eddystone, PA

DRS Daylight Defense, LLC
San Diego, CA

DRS Laurel Technologies
Largo, FL

DRS Power and Control Technologies, Inc.
Milwaukee, WI

DRS Sustainment Systems, Inc.
West Plains, MO

Eutelsat America Corp
Washington, DC

General Atomics Aeronautical Systems, Inc.
Palmdale, CA

General Dynamics Mission Systems, Inc.
Scottsdale, AZ

HII Mission Driven Innovative Solutions, Inc.
Huntsville, AL

Honeywell International, Inc.
Clearwater, FL

iGov Technologies, Inc.
Reston, VA

Kearfott Corporation, Guidance & Navigation Division
Woodlawn Park, NJ

L3Harris Technologies, Electron Devices, Inc.
Torrance, CA

L3Harris Technologies dba Datron Advanced Technologies
Simi Valley, CA

LGS Innovations, LLC
Westminster, CO

Lockheed Martin Corporate Headquarters
Bethesda, MD

Lockheed Martin Government Affairs
Arlington, VA

Lockheed Martin Missiles and Fire Control
Camden, AR

Lockheed Martin Rotary and Mission Systems
Orlando, FL

Lockheed Martin Rotary and Mission Systems
Mitchel Field, NY

Lockheed Martin Rotary and Mission Systems
Moorestown, NJ

Lockheed Martin Rotary and Mission Systems
Marinette, WI

Lockheed Martin Sippican, Inc.
Marion, MA

Lockheed Martin Space
Washington, DC

Lockheed Martin Space
Huntsville, AL

Mercury Systems, Inc.
Andover, MA

NEXGEN Communications, LLC, a wholly-owned subsidiary of L3Harris Technologies, Inc.
Sterling, VA

Northrop Grumman
Irving, TX

Northrop Grumman Space Systems Military & Civil Space, Azusa
Azusa, CA

Peerless Technologies Corporation
Fairborn, OH

Polaris Alpha Advanced Systems, Inc.
Fredericksburg, VA

PreTalen Ltd.
Beavercreek, OH

Raytheon Company
Aurora, CA

Raytheon/ Lockheed Martin Javelin Joint Venture
Tucson, AZ

Robotic Research, LLC
Clarksburg, MD

Rolls-Royce North America Inc. Washington, D.C. Office
Reston, VA

Science and Technology Corporation
Hampton, VA

Tactical Engineering & Analysis, Inc.
San Diego, CA

Tech Wizards, Inc.
Newburg, MD

Thales Defense and Security, Inc.
Clarksburg, MD

The Texas A&M University System
College Station, TX

Toyon Research Corporation
Goleta, CA

Trident Research, LLC
Austin, TX

Viasat, Inc.
Carlsbad, CA

Virginia Polytechnic Institute and State University
Blacksburg, VA

Zimmerman Associates, Inc.
Washington, DC

IN THEIR OWN WORDS

A representative sampling of the 2020 Cogswell winners were invited to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high-quality security posture.

ACUITY, INC.

By Tracy Wright, Bryan Prewitt, Elan Keene, and Kaitlyn Ernstmann

Acuity, Inc. is a consulting firm headquartered in Reston, Virginia, with a focus on providing technical solutions to federal agencies supporting the national security and public safety missions. We are honored to be selected for our first James S. Cogswell Award. This momentous achievement would not have been possible without the support of Acuity's senior leadership, employees, and dedicated security team. In addition to our strong partnership with DCSA, we identified three areas that made the biggest impact in our blueprint for winning a Cogswell Award: our standards and practices, our leadership and employee buy-in, and our desire to continually go above and beyond.

RIGID ON STANDARDS, FLEXIBLE ON PRACTICE

We strictly adhere to standards established through federal regulations (including the National Industrial Security Program Operating Manual), executive orders, and guidance from DCSA; however, we make it our mission to provide our employees with flexibility to complete their tasks. One such flexible measure is offering self-paced initial and refresher briefings, distributed at the appropriate intervals. Additionally, all employees are invited to attend our monthly new employee orientation, at which our security team presents our initial brief. We also acknowledge employees' constraints and work to prevent redundancies by accepting government trainings. For example, we require all employees to complete a cybersecurity training course, but if an employee completes training associated with his/her current client, we accept such training.

BUY-IN

At Acuity, adherence to security policies, procedures, and practices is inherently important to senior leadership. Leadership maintains an open-door policy and continued support, whether that is discussing security reform, researching technological advancements (automated software), or offering sponsorship to professional organizations, like NCMS (the Society of Industrial Security Professionals). Additionally, the security team is invited to attend and participate in corporate, business unit, senior management, and quarterly leadership meetings to ensure effective communication and strong rapport between departments. In addition to leadership's support, an overwhelming majority of our employees understand and appreciate the significance of our security program and are happy to assist whenever requests are made.

GOING ABOVE AND BEYOND

The security team is constantly reviewing our program to identify areas where we can improve. In the past few years, we have worked closely with our DCSA representatives to make our security vulnerability assessments more streamlined. We have also required all employees to complete Insider Threat Awareness (ITA) training via the Security Training, Education and Professionalization Portal (STEPP).

To stress ITA importance, we hosted our first annual ITA Month/Day in September 2019. Throughout the month, we distributed ITA information, and on the chosen ITA Day, we hosted all-day activities for employees in person

as well as remotely. ITA Day activities included a discussion of real-life insider threat examples, facilitated by Acuity founder and CEO Rui Garcia, followed by a series of informational videos, group discussions, games, and prizes.

We also require all employees going on foreign travel to complete a four-step travel reporting process. Employees are required to complete a travel notification briefing prior to travel. Upon return, they have to complete a debriefing, both written and verbally. Additionally, throughout this reporting process, screening for foreign contacts and export compliance standards are intrinsically intertwined.

In closing, we are honored to accept our first Cogswell Award on behalf of our entire Acuity family. We would not have achieved this award without our DCSA partners and our dedication to security excellence.

AMERICAN SYSTEMS

By April Ortiz, Facility Security Officer, Albuquerque Office, New Mexico

WHO WE ARE

Founded in 1975, AMERICAN SYSTEMS provides enterprise information technology, acquisition and lifecycle support, engineering and analysis, test and evaluation, and training solutions to the Department of Defense (DoD), Intelligence Community (IC), and civilian government customers. We are one of the top 100 employee-owned companies in the United States, with approximately 1,400 employees nationwide. We are based in Chantilly, Virginia, with satellite offices throughout the country.

I have served as the facility security officer (FSO) for our Albuquerque office for the last five years. I had been working in the security department for several years when I became a first-time FSO in 2015. Prior to that, I had the privilege of working with some of the best in the field. While I came into the job with a solid security background, I decided to enhance my knowledge by taking the "Getting Started Seminar for New FSOs" course at the Center for Development of Security Excellence (CDSE). This was a great experience for many reasons, particularly for the practical knowledge I gained and the opportunity to network with other new FSOs. Over the last few years, my knowledge grew with our program. I am now happy to give back to the security community that supported me by mentoring, serving on the board of our local Society of Industrial Security Professionals (NCMS) enchantment chapter, and being a resource to my fellow FSOs.

OUR PROGRAM

The AMERICAN SYSTEMS Security Department's vision is to become the standard by which companies build their security programs. This is accomplished by establishing efficient processes and procedures, utilizing technology to its fullest potential, and hiring, retaining, and training a highly talented security staff.

Utilizing this vision, taking what I have learned, and building on the foundation of a great program, I proceeded to take our program to the next level. I implemented comprehensive security education, which involved reinforcement of security best practices, employee involvement, and close coordination with our local DCSA representatives. Since then, our facility has consistently achieved the highest security ratings.

Running an effective security program requires many elements. We have found that an integral part of a successful program is working in conjunction with our DCSA representatives. They provide invaluable information, support, education, and guidance. This was imperative when we transitioned to DCSA's new risk-based methodology. At that time, with DCSA feedback, I developed a threat analysis report that consolidated all pertinent threat and risk mitigation for a

contract into a user-friendly format for easy review. This was shared with our local NCMS chapter and the local security community. Furthermore, having our local representatives from DCSA, counterintelligence, and FBI provide briefings makes security real for our employees. It helps them understand that security is a daily job and not an abstract concept.

Another vital piece to success is active involvement in our NCMS chapter. We depend on our local NCMS chapter to bring us the latest security information, connect us with our local security community, and offer relevant training.

I believe strength comes from within. It is essential to have a cohesive, supportive security team. Our corporate security director has brought our security department together into a solid supportive entity. Everyone in our department knows they can call on any one of their teammates to provide support, mentoring, and/or knowledge. Our local security staff are dedicated professionals with an eye on the vital work we do in protecting national security information. Our information system security manager developed forms and scripts and provides in-depth training for all users of our accounting information system to enhance our security awareness.

Finally, without the support of corporate security on programs such as peer reviews, robust insider threat education/training, foreign travel risk awareness/education, and phishing exercises, our effectiveness would be challenging. All these programs promote an awareness of National Industrial Security Program Operating Manual (NISPOM) compliance and employee security responsibilities within AMERICAN SYSTEMS

IN CLOSING

Our recipe for success involves many moving parts, including collaboration with our DCSA representatives, unwavering support of our senior management, security-educated employee owners, corporate involvement on security issues, and a culture of joint accountability.

The honor of this James S. Cogswell Award is a first for AMERICAN SYSTEMS. I am confident it will not be the last as we continue to strive to meet the ever-changing challenges of our security environment. We know what's at stake.

ASM RESEARCH

ASM Research
An Accenture Federal Services Company

By Orlando Ferreiras, Vice President and Facility Security Officer

ASM Research, an Accenture Federal Services company, is a leading solutions integrator focused on using information and technology to solve real-world problems for the federal agencies we serve. Our employees apply the latest technologies and practices in systems modernization, workforce development, infrastructure support, and operations security to help our clients meet their challenges in force structure, training, healthcare, security, and education. For more than 40 years, our commitment to our clients' missions has repeatedly produced extraordinary results.

We are honored to receive the Cogswell Award, as it recognizes our commitment to making security a priority while protecting our nation in these difficult times. Our security program's success can be attributed to leadership commitment, our security organization, our relationship with DCSA, and our training and testing program.

LEADERSHIP COMMITMENT

The success of our security program rests largely on our employee leaders, who are always seeking new ways of keeping our company and our country safe and secure. Our dedication to searching for the right thing to do, and overcoming the challenges to execute on that vision, are the key to our success. Our executive leaders and employees are committed to our culture and each other's success, with decades of service to our company that allows continuous process improvement with a strong understanding of past failures and successes.

We operate in an inspection-ready environment at all times because the bad actors are not going to announce their actions. Because we have built a culture of trust, our employees lead the way to improving client's operations and our security program. They provide valuable feedback and recommendations that makes us all better. They define their vision for the future, get others on board, and follow the path of excellence.

SECURITY ORGANIZATION

ASM Research was established in the Pentagon basement in 1978, when the company's founder and two employees programmed a small system to support soldier training for the U.S. Army. Our president, John Fraser, supported me in formalizing our security organization in the early 2000s. The mission was to integrate security into our culture, programs, and practices while meeting the highest security standards. We hired strong leaders to build a meritocracy based on knowledge, mutual respect, trust, and leadership. Our organization is responsible for security across the company. All business units report directly to me, which allows for transparency, greater employee retention, and effective risk management.

KEY RELATIONSHIPS

While always good, our relationship with DCSA became a true partnership when Paul Busenberg was assigned as our DCSA representative. He took the initiative to teach us where we could improve and was always available to provide mentoring and guidance. Our strong relationships with our parent company leaders and security organizations across government and industry help us validate our thoughts and processes, which help us deliver better services to our employees and clients.

TESTING AND TRAINING PROGRAM

A major pillar of our program is constant testing to validate our assertions and processes and then sharing the results with all employees so they can see for themselves how we are performing in certain areas and where our culture can improve.

BAE SYSTEMS

By Dave Cheney, Facility Security Officer

The Electronic Systems (ES) sector of BAE Systems, Inc. is a global leader in researching, developing, implementing, and maintaining cutting edge commercial, defense, and space electronics. BAE Systems ES is dedicated to the success of its customers and places security as a top priority in protecting the nation's most sensitive programs.

The success of our security program can be attributed to several factors: a robust self-inspection program, leadership support, standardization of security policies and practices, communication, and collaboration with DCSA, and strong special security agreement (SSA) guidance regarding foreign ownership, control, or influence (FOCI) mitigation. Receiving the Cogswell Award for three of our BAE Systems ES facilities underlines our commitment to the SSA and the success of our customers.

"I am extremely proud of the hard work and commitment the entire BAE Systems ES security team demonstrates on a daily basis, ensuring the protection of our nation's most sensitive information," said Brian Mackey, vice president of ES Security at BAE Systems. "We are privileged to receive this award at these three locations, as confirmation of the teams' efforts."

ROBUST SELF-INSPECTION

Our security team understands the importance of formal annual self-inspections. Self-inspections are broken into sections and assigned to security team members by the facility security officer (FSO). Many BAE Systems facilities have subject matter experts (SME) in discipline areas such as communications security (COMSEC), physical security, education, and training, etc. These SMEs are knowledgeable in National Industrial Security Program (NISP), industrial security letter

changes, and can often identify and correct vulnerabilities unknown to the untrained eye.

Additionally, ES has developed a staff assistance visit program conducted by non-resident BAE Systems security staff who lead internal reviews and provide an additional set of eyes during inspections. A fresh set of eyes can often see an issue that otherwise might go unnoticed. BAE Systems strives for complete and meaningful adherence to the protection and safeguarding of classified materials as well as building employee awareness and program effectiveness through enhancements and sharing best practices among the entire cleared defense contractor community.

IT TAKES A VILLAGE

A successful security program is represented by many disciplines. Each FSO is responsible for overall management, but successful compliance cannot happen without the support of a larger team. BAE Systems ES has multiple disciplines to include personnel security, COMSEC, centers of excellence, our Proprietary Alarm Monitoring Center, and a strong information assurance team. This structure greatly supports standardization and allows us to efficiently adjust to regulation changes.

The ES sector takes experience and lessons learned from each security officer to share within the industrial security community. Through these individuals, we collaborate with our local DCSA agents, while contributing to the strength of our relationships to the local field office.

PARTNERSHIP

The success of our security program is due to the partnership we've established with DCSA. The strong relationship that exists between the local site security team and security management has been noted by DCSA. BAE Systems ES is well-known as a superior reporter of suspicious contact reports and insider threat incidents, which is an indicator of the overall effectiveness of our security and counterintelligence programs. BAE Systems ES' insider threat program is a tiered approach that extends to senior management within the organization. Sharing information and being an active member within the NISP community is an important part of what we do. Managing a robust relationship with senior management and maintaining a strong security team are the ingredients necessary to build and manage a successful security program.

DRS POWER

By Thomas Clark, Facility Security Officer

Training and leadership involvement are the two key elements of success for Leonardo DRS Power & Control Technologies, Inc. in Milwaukee, Wisconsin. As the facility security officer (FSO), I always tell our employees that they are the security program — the FSO is just the point of contact for the government. My hope is to instill ownership of the security program within each employee.

Many of our employees have never worked for a defense contractor nor had any prior government experience. The ownership baton is initially passed at new hire training. That first meeting — and first impression of the security program — is fundamental to the long-term success of the program. Getting buy-in on the importance of protecting our government customers' information at this point is the cement that holds the program together. This initial training is paramount to the multiyear success of the company's security program. Our facility is big — there is only one FSO for a headcount of over 600 and enlisting the employees as security helpers is essential.

After their new hire training, the FSO provides focused training at various times throughout the year, including training specific to business development, foreign travel, and insider threat to further increase employees' knowledge base. This battle rhythm culminates with an annual security fair.

In addition to providing employees with a strong knowledge base for security, support from management is also crucial to an affective and successful security program. Long term success in any organization cannot be sustained without management support. Security needs to have a seat at the table, it needs to be part of the leadership team. In order to plan, program, and support business needs, security has to be at the forefront of the process and not an after-the-fact necessary evil. Leadership buy-in promotes a security conscience throughout the entire organization.

The elements of training and leadership can provide a continuous flow to any security program, keeping the entire organization in sound security practices.

JAVELIN JOINT VENTURE

By Marek Wolert, President and Tom Broka, Facility Security Officer — Javelin Joint Venture

The Javelin Joint Venture (JJV) is a partnership between Raytheon Missiles & Defense and Lockheed Martin Corporation, created to provide, maintain, and upgrade the Javelin Weapon System for the U.S. Army and customers worldwide. The Javelin is a versatile, one-man portable and platform-employed fire-and-forget anti-tank weapon system. To date, we've produced more than 45,000 missiles and 12,000 command launch units, and it is expected to be in the U.S. military's operational inventory through 2050. We continue to be proud of our ability to bring the Javelin's capabilities to our nation's warfighters.

As the recipient of two James S. Cogswell Awards in the last five years, Raytheon/Lockheed Martin Javelin Joint Venture Corporation – Tucson, Arizona, has clearly demonstrated its commitment to protecting national security, the warfighter and supporting the mission of DCSA.

We are honored to be chosen as recipients of the Cogswell Award. It is a recognition of the hard work and dedication of our Javelin Joint Venture and its commitment to protecting our nation's assets. JJV understands that effective security requires true partnership with DCSA and a comprehensive security program with a full organizational commitment that encompasses each of its key elements: industrial security, information security (cyber), physical security, insider threat, and counterintelligence. "We could not be as effective in our security program without the collaboration of our local DCSA partners and many security professionals at Raytheon," said Tom Broka, JJV's facility security officer (FSO).

PARTNERSHIP WITH DCSA

"I can pick up the phone anytime and have a candid conversation with my local industrial security representative, Mike Rudzinski, which leads to open and honest communication." said Broka. JJV also leverages a partnership with Raytheon Technologies and employs interactive security tools to foster information exchange and collaboration among security professionals and key stakeholders. JJV also looks outside the company and actively seeks external information, training tools, and other resources from leading industry organizations like NCMS (the Society of Industrial Security Professionals), the Center for Development of Security Excellence (CDSE), and the local industrial security awareness council.

MANAGEMENT SUPPORT

Both program and management support to the security program is the important first step in having a strong program. Without that essential leadership and influence, our security program would not be at such a high level of compliance. Leadership helps influence and shape the security culture within our company. Their

regular weekly staff meetings and quarterly all-hands point and aim at the latest areas of emphasis. Continuous education refreshes proper security procedures, allows us to focus on current security challenges, and highlights mistakes that the employees can relate to and learn from. "The capability that we provide and manage requires us to maintain a heightened state of diligence in order to protect our nation's critical information, and in turn, our warfighters tactical advantage," said Marek Wolert, Javelin Joint Venture president. "We've partnered with our sponsors, and together we've enabled our team and processes to meet or exceed security standards."

EMPLOYEE PARTICIPATION

Ultimately, the true reflection of our security program relies on employees. We implement security compliance with security procedures, but if we didn't educate on a regular basis and drive the culture, the security program would not be at such a high level. We have made it a point for our employees to report to us with the "see something, say something" mentality. It took years to build that relationship and culture, and it has been paying off in big dividends throughout the last 10 years. We make it a point to conduct walkabouts and get away from our desks to conduct employee security interviews. It has been very effective with the one-on-one interviews. Employees feel comfortable, and that has really opened up a line of communication that was not always there. Continuous engagement is key, resulting in effective reporting obligations such as adverse information and/or insider threat concerns. They are the eyes and ears of the security program — tremendous in helping report any counterintelligence concerns they may encounter.

DELIBERATE WITH CONSISTENCY

Overall, achieving superior ratings requires being consistent and all-in with security. We plan various educational events throughout the year, trying our best to make it interactive and answering employee questions as a group. This has really been effective, fun, and promotes some competitiveness amongst the group. We also have security physically embedded with the employees within the program. This gives us the availability to build a great partnership with employees and leadership. We invite speakers from various agencies to discuss topics of threat reporting, counterintelligence threat briefs, and threat management training. Without the team effort, superior ratings would not be possible. It is such an honor to accept the Cogswell Award on behalf of the Raytheon/ Lockheed Martin Javelin Joint Venture Corporation in Tucson, Arizona.

LOCKHEED MARTIN

On behalf of the entire Lockheed Martin security team, we are honored to receive 10 James S. Cogswell Awards this year at the following facilities:

Rotary and Mission Systems - Marinette, WI	FBM Liaison Office - Washington, DC
Lockheed Martin Sippican Inc. - Marion, MA	Corporate Headquarters - Bethesda, MD
Rotary and Mission Systems - Mitchel Field, NY	Government Affairs - Arlington, VA
Rotary and Mission Systems - Moorestown, NJ	Missiles and Fire Control - Camden, AR
Rotary and Mission Systems - Orlando, FL	Lockheed Martin Space - Huntsville, AL

We are very grateful for the recognition of the hard work, dedication, and innovation of our security professionals. In partnership with DCSA, we at Lockheed Martin strive to achieve security excellence across our entire company. This partnership allows us to deliver uncompromised technology and platforms to the

warfighter. The ability to do that rests with the engagement and effectiveness of our security professionals, in tandem with our government partners at the local and national level. This is our daily goal.

In their pursuit of excellence, security programs across Lockheed Martin seek continuous improvement through identification of innovative methods. Mere compliance is not the goal. These efforts are evident in our security programs and can be found in every discipline, including operations and compliance, classified cybersecurity, physical security, international security, counterintelligence, and of course the cornerstone of all security programs — security education and awareness. Each year, the security team evaluates the success of existing goals and identifies new goals, with a focus on continuous improvement. This effort directly contributes to the standard of excellence our security programs consistently achieve.

This achievement would not be possible without the support and collaboration of two important stakeholders: the dedicated employees of Lockheed Martin, and our primary government oversight customer, DCSA. Lockheed Martin security professionals work side-by-side with our government counterparts at every level to ensure more than compliance. From the ongoing partnership with the local industrial security representative, counterintelligence special agent, and information system security professional, to the availability and engagement with the field office chiefs, authorizing officials, and regional directors, all the way to the senior leadership of the agency, their doors are always open, which fosters success. We share ideas and work together at every level to advance the National Industrial Security Program (NISP).

Our teamwork results in the ability to address and resolve challenges beyond what impacts Lockheed Martin, but what benefits the industrial security community at large. Our commitment to this partnership is seen in many forms of engagement, from collaborating within government working groups, serving on industrial panels, and sharing the voice of industry at the government policy table. That trust and support is mutual, and we work together with DCSA to formulate requirements and methods of applying new standards that truly improve the security of our nation's secrets. In doing so, we shape the future together. We face these challenging times together, and we are committed to delivering a program that is effective and is second to none. We thank DCSA for their trust in us and their day-to-day teamwork to make these security programs successful.

NEXGEN

L3HARRIS™ FAST. FORWARD.

By Tammi Shapiro, Director of Security and William Winkler, Senior Security Manager

L3Harris Technologies is a proud member of the defense industrial base and has a strong history with DCSA, as evidenced by the company's 16-year track record of Cogswell Awards.

This level of success stems from strong support at all levels, establishing a culture of security and continuous improvement and creating a true partnership with DCSA.

L3Harris' security program is supported from the highest level of company leadership, including the corporate security officer, along with the regional company and DCSA representatives.

The security organization actively incorporates feedback and best practices gleaned from past inspections and knowledge shared among in-house inspectors and others from across the corporation. Security teams at the company's individual sites collectively leverage their years of experience from different markets and apply their joint knowledge in growing the company's security posture.

Teamwork is essential when building a strong security program because it's not just about what security itself can do, but also about collaborating across the entire business to create a culture of security conscious individuals. Our Sterling, Virginia, location epitomizes L3Harris' security culture. It does not matter who is wearing what hat — from our facility security officer (FSO) to our program managers — security is everyone's business.

The company also routinely pressure tests its security protocols and follows a model of continuous improvement. Security representatives incorporate feedback from employees to ensure they enable the business without compromising security standards. These spirited engagements result in improved processes and a strong partnership across the business and customers.

This was evident in a few of the specific areas our DCSA representative highlighted this past period:

- An enhanced visit inspection plan for the front lobby, incorporating a random scheme that produces 100% inspection for selected employees in addition to 100% inspection of visitors.
- A security daily risk report captures threat data relevant to sites, technologies, and employees.
- Foreign travel briefings given to cleared and uncleared employees. Custom briefings are generated using briefing data, as well as State Department and corporate international travel websites.

The company's partnership with DCSA is invaluable in making a strong security program. DCSA representatives are aligned within the company's teams, providing direction and encouragement to take the program to the next level — sharing in the team's continuous improvement mentality. When security representatives showcased their enhancements and improvements during a continuous monitoring meeting, the DCSA representative shared in their excitement.

The company's DCSA representatives are an integral part of the security heritage and culture, and through their partnership, L3Harris is fortunate enough to receive this prestigious award.

NORTHROP GRUMMAN CORPORATION, AZUSA FACILITY

By Renee Jeleniowski, Communications Representative and Mike Musquiz, Facility Security Officer

Northrop Grumman is a global aerospace, defense, and security company. The majority of our business is with the U.S. government, principally the Department of Defense (DoD) and Intelligence Community (IC). In addition, we deliver solutions to global and commercial customers.

At Northrop Grumman, Azusa, California, our key responsibilities include infrared payload development, mission data processing, and information assurance for both military and civil restricted programs, and we have one of the most complex security programs within our sector. Despite this complexity, the Azusa site received a near perfect score on its recent DCSA assessment, resulting in a second superior rating and securing our eligibility for the prestigious Cogswell Award.

To be chosen as a 2020 Cogswell Award recipient is a feat that would not have been possible without our entire team— our village of support — ensuring the success of the security program's critical mission to protect our nation's classified information and programs that protect the warfighter.

LEADERSHIP

Successfully enforcing a security awareness program does not happen without the active participation of the leadership team. Our leadership team continuously offers unwavering support throughout our entire

security awareness process, from the initiation to the execution. Leadership's active engagement in security education and training events sends a positive message to the campus about the importance of our security program.

PROGRAM AND EMPLOYEE PARTICIPATION

In 2019, Northrop Grumman, Azusa's Space Based Infrared System's Contractor Logistics Support Program was selected to participate in an enhanced security vulnerability assessment (eSVA). The program management team played a critical role in preparing the business process and asset identification information. The commitment by the team was essential to showing how the Azusa site protects a program that is vital to the interest of the nation.

Azusa employees are the key to the success of our security program. An employee's constant involvement with the security program is what makes the program efficient and effective. We are pleased with how our employees exhibited their understanding and readiness to be compliant with security policies and procedures.

DCSA PARTNERSHIP

For many years, Northrop Grumman has worked alongside DCSA, building a true partnership and establishing a culture of strong cooperation through open lines of communication, which proved to be instrumental in the success of our security program. We are so grateful for our industrial security representative — Mark Jones from DCSA — who has been an integral part of our team's success.

SECURITY TEAM

The Azusa security, industrial, and cyber teams have educated the Azusa site on the vital role they play as dedicated security professionals to carry out our mission on a daily basis. With developing plans, creating schedules, providing creative ways to deliver security education, self-inspecting, and interacting with DCSA, the Northrop Grumman, Azusa security team has done an outstanding job.

CREATING A SECURITY COMMUNITY

When building an effective security community, there are a few key considerations. They include ensuring our employees receive an annual refresher briefing, allowing security to have a seat at the table with leadership, communicating regularly and often with the employees regarding security policy and procedures, conducting security education and awareness events, working with programs to stay ahead of emerging threats, and collaborating with DCSA and other government agencies.

IN CLOSING

The collaboration that seamlessly occurs between each of these entities is truly remarkable and ensures we are integrating security knowledge and awareness in all disciplines. To receive the Cogswell Award not only shows the strength we demonstrate within our security posture, but it also strengthens the Northrop Grumman reputation of being a top performer in our industry.

PRETALEN

By Julie Mannheim, Facility Security Officer

CONSTELLATION OF INNOVATION

PreTalen, the go-to engineering firm for superior cyber engineering and position, navigation, and timing solutions, was acquired by Centauri in late 2019. Our national network of teams focuses on providing expert systems engineering support for space, navigation, electronic warfare, and cyber security.

We are excited to be a part of Centauri — a high-end engineering, intelligence, cybersecurity, and advanced technology solutions company, headquartered in Chantilly, Virginia, with offices nationwide. Centauri works with customers in the intelligence and national security communities, helping them solve their most difficult challenges. Centauri's agile, mission-first approach empowers advanced technical and

operational teams to meet the real-time demands and high-impact missions of national defense agencies across land, air, sea, space, and cyberspace.

TRAINING NEVER ENDS

As soon as I joined PreTalen as facility security officer (FSO), I was given an open door, and through that door I went — organizing, creating, and communicating with the team and management. I already had the applicable training courses levied by DCSA, as outlined within the National Industrial Security Program Operating Manual (NISPOM), and by other contracting government agencies; However, training never ends in this field. Changes are always upon us.

MENTORSHIP

During my career, I have mentored more than seven FSOs throughout the Dayton, Ohio, area and neighboring communities. I have unofficially mentored a few as well. In my experience, mentorship tends to trickle down. I learned so much from my mentors over the years and have passed that knowledge on to my mentees. My hope is that these lessons continue to be passed on, from FSO to FSO, from mentor to mentee.

Mentorship is important to growing the FSO profession. My advice to those just starting out is to take as much learning and input as you can from those that have the knowledge and are willing to teach you. Knowledge is one of the best gifts to give – it's thoughtful, free, and regifting is encouraged!

COMMUNICATION IS KEY

When I joined PreTalen, the company was a non-possessing facility with a small, dedicated team. Within a year, we had processed a ton of hires out of college and upgraded the facility to possessing classified information, and within the next few months after that to a facility processing classified information. I'm proud of what we accomplished in such a short time. This could not have been done without the communication with our DCSA representative and their team. They helped with numerous questions, paperwork reviews, and on-site assist visits. This communication and collaboration helped our security posture and our facilities security program.

We're proud to win the James S. Cogswell Award — it shows that training, mentorship, and communication is vital to a security program and that true collaboration between industry and government is essential to ensure the protection of classified information, materials, and programs.

ROBOTIC RESEARCH

By Janet Hughes, Facility Security Officer

Equally important to holding a facility clearance is the responsibility that goes along with the honor of doing business with the Department of Defense in support of America's frontline warriors. My company views our facility clearance as both an incredible opportunity but also an awesome responsibility. Nothing less than the lives of our men and women in uniform are on the line. To protect them, we must protect our nation's secrets, along with our company's intellectual property and our people. Training provides a strong path to that protection.

Increasingly, this is where the main fight for future battlefield dominance is taking place — in small companies like ours, with potentially game-changing technology. America's adversaries have been able to cut years, perhaps decades, off the time it takes to develop new capabilities by stealing America's secrets. It's a battle every day to safeguard our intellectual property (IP) — the lifeblood of our company and so many others.

I am lucky — my executive team backs my security program to the fullest. We are a very small, very dynamic company, and we all wear many hats. The support I

have received from my executive team has enabled me not just to "minimally comply" with DCSA and DoD directives and instructions, but to go well beyond that. We believe in complying with both the letter and the spirit of the security regulations and instructions from our customers.

Like DCSA, Robotic Research places enormous value on its people, and we know that the human dimension is an increasingly important "front" in the battle to secure our nation. That's why we work hard to educate and train our people monthly, and in varying formats, to avoid training boredom and protect our people. They, too, are primary targets by adversaries seeking to exploit any perceived weaknesses. Whether in cyber hygiene or personal behaviors, we must always be on the lookout for insider threats, and that makes insider threat training one of my continual top priorities.

Of course, I know my company cannot secure our IP and our people alone. It is only through a genuine partnership with DCSA and others that we will win the battle. We have been blessed to have had the privilege of working with some of the finest counterintelligence and security analysts in the world. And we know that when we call with questions or issues, we will be respected and treated professionally. What a great partner DCSA has been to Robotic Research!

VA TECH

By John Talerico, Office of Export and Secure Research Compliance Director, Office of Research and Innovation

Virginia Tech's Office of Export and Secure Research Compliance (OESRC) ensures university-wide compliance with export controls, sanctions, and industrial security laws and regulations. As a business unit within the Virginia Tech Office of Research and Innovation, it promotes fundamental research, protects U.S. technology, and seeks to educate Virginia Tech employees and students about regulations and requirements on Virginia campuses in Blacksburg and Roanoke, Virginia. It is expanding operations into the greater Washington, DC metro area as Virginia Tech's presence and national security research continues to grow in that region.

Virginia Tech's industrial security program is now a three-time national award recipient of DCSA honors. In addition to this 2020 James S. Cogswell Outstanding Industrial Security Achievement Award, our program received the DCSA Award for Excellence in Counterintelligence in 2018 and our first Cogswell Award in 2016. We are greatly honored by the recognition of our commitment to protect classified information and our national security.

DAY-TO-DAY OPERATIONS

OESRC engages in a number of activities across the Virginia Tech community for the benefit of our security program, including reviewing and providing guidance on agreements, gifts, invention disclosures, conflict of interest disclosures, international visitors, and international graduate student applicants. OESRC also provides an extensive training program for both cleared and uncleared researchers and administrators as well as direct services to these customers for all controlled unclassified and classified information security.

PARTNERSHIP AT ITS BEST

In February, Virginia Tech was one of 10 universities selected to participate in the DCSA CI Academic Outreach program with goal of developing a stronger relationship with the agency, focusing on the needs of academia, and providing a forum to generate and test new information or processes that can then be shared with the broader cleared university community.

Our program would not be Cogswell caliber without the exceptional partnership we have with our DCSA representatives: Industrial Security Representative

Garrett Speace, Counterintelligence Special Agent Michele Yoworski, and Information Systems Security Professional Keith Wagner. We consider them an extension of our team, as they are always responsive and willing to provide guidance to us when we need them, especially during the COVID-19 pandemic.

SENIOR MANAGEMENT SUPPORT

Unwavering support from senior management and leadership has been essential to the security program, and it has enabled the security program to function with a high level of autonomy, assurance, and leadership responsiveness to program needs. We have the ability to hire experienced staff who are security conscious, focus on training professional development, and continue to strengthen the partnership with DCSA and other government agencies. Most importantly, we stay engaged with our internal community, peers, and leadership.

CONTINUOUS IMPROVEMENT

As Virginia Tech continues to grow, it is even more important that the security program is proactive and does not wait for an assessment to measure its effectiveness. We continuously evaluate all aspects of our program, including personnel clearance actions, facility operations, standard practices and procedures, contract reviews, and information security tools to ensure we are operating in a manner that is both compliant with the National Industrial Security Program Operating Manual (NISPOM) and other policy documents and maximizes efficiency and security. We stay abreast of DCSA's tools and information as they evolve and participate in trainings, review and leverage counterintelligence information, and keep regular contact with DCSA representatives.

All of these measures are taken to provide a safe and secure environment for our faculty, staff, and students to conduct national security-related research for the advancement of our defense and intelligence capabilities. While we are extremely honored by the 2020 Cogswell Award, our team does not consider our job done. We continue to strive for the strongest security program possible and make sure we earn the distinction as a Cogswell Award recipient each and every day.

VIASAT

By Joyce Johnson, Senior Security Director and Insider Threat Program Senior Official

Viasat is extremely honored to be a recipient of this year's James S. Cogswell Award. We realize this prestigious milestone could not have been achieved without the partnerships and commitment of every employee, our management team, and the exceptional relationship we have with DCSA.

Viasat is a global communications company, bringing connectivity to businesses, residents, militaries, airlines, and populations — anywhere. With deep roots in defense, Viasat is emerging as a national asset to government, the Department of Defense (DoD), Intelligence Community, and coalition forces around the world.

Over the past 30 years, Viasat has grown to be a market leader in the areas of next-generation tactical datalinks, cybersecurity and information assurance, satellite communications (SATCOM), and the design, development, and manufacture of next-generation, high-capacity satellites. Our security program is an important element of this success.

INNOVATIVE SECURITY LEADERSHIP

At Viasat, our passion, determination, and innovative culture drives everything that we do, and we approach security in the same way. Our call to action says it all: "do the right thing." These four simple words carry a big punch. Our senior leaders are passionate about security and have made it a top priority, actively engaging in our education program and routinely participating in our security initiatives. They help to shape our security culture and set high expectations.

PARTNERSHIPS AND TRANSPARENCY

Our success is built on internal and external partnerships. Employee participation is crucial, and all employees act as security ambassadors. There is a trust built between the security team and our employees. When problems arise, we work together on a solution that meets compliance and allows our creative workforce to meet their objectives. We rely on transparent, open dialogue, knowing we are all trying to "do the right thing."

Our partnership with the DCSA San Diego Field Office has been crucial to developing a strong, compliant program. We can pick up the phone and talk through any issue or idea with the confidence that we are all working towards a common goal of protecting information. The counterintelligence group within DCSA is an important aspect of keeping our company's security posture strong and developing a two-way line of communication is a must. We encourage all cleared defense contractors to report, report, report and to use the feedback from DCSA as a building block to education.

Get involved with partners such as Industrial Security Awareness Council and NCMS (the Society of Industrial Security Professionals) to develop working groups with other cleared industry, and share your challenges and successes with others.

EDUCATION

A cross-functional education program is the backbone of a strong security program, and it starts on day one for all new employees. We strive to bring fun, innovation, and consistency to our training platforms. Educated workforces support every element of security.

TEAM COMMITMENT

One of the most vital aspects of a great security program is your team, and we are blessed to have an incredibly dedicated and professional group of people that possess a passion for what they do. Encourage your teams to never stop learning, try new things, not be afraid to fail, and always "do the right thing."

We encourage every security professional to take the time to appreciate the value you bring to your company and the important job you are doing to protect our nation, our warfighters, and your employees. Thank you to all who participate in the selection process for this prestigious award. Viasat is truly humbled to be part of this amazing industry.

Brig. Gen. Arthur E. Exon (left), director of the Defense Contract Administration Services, presents the Cogswell Award to Dr. John B. Smyth (right), president of Smyth Research Associates on February 14, 1967.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil

571-305-6562

www.dcsa.mil