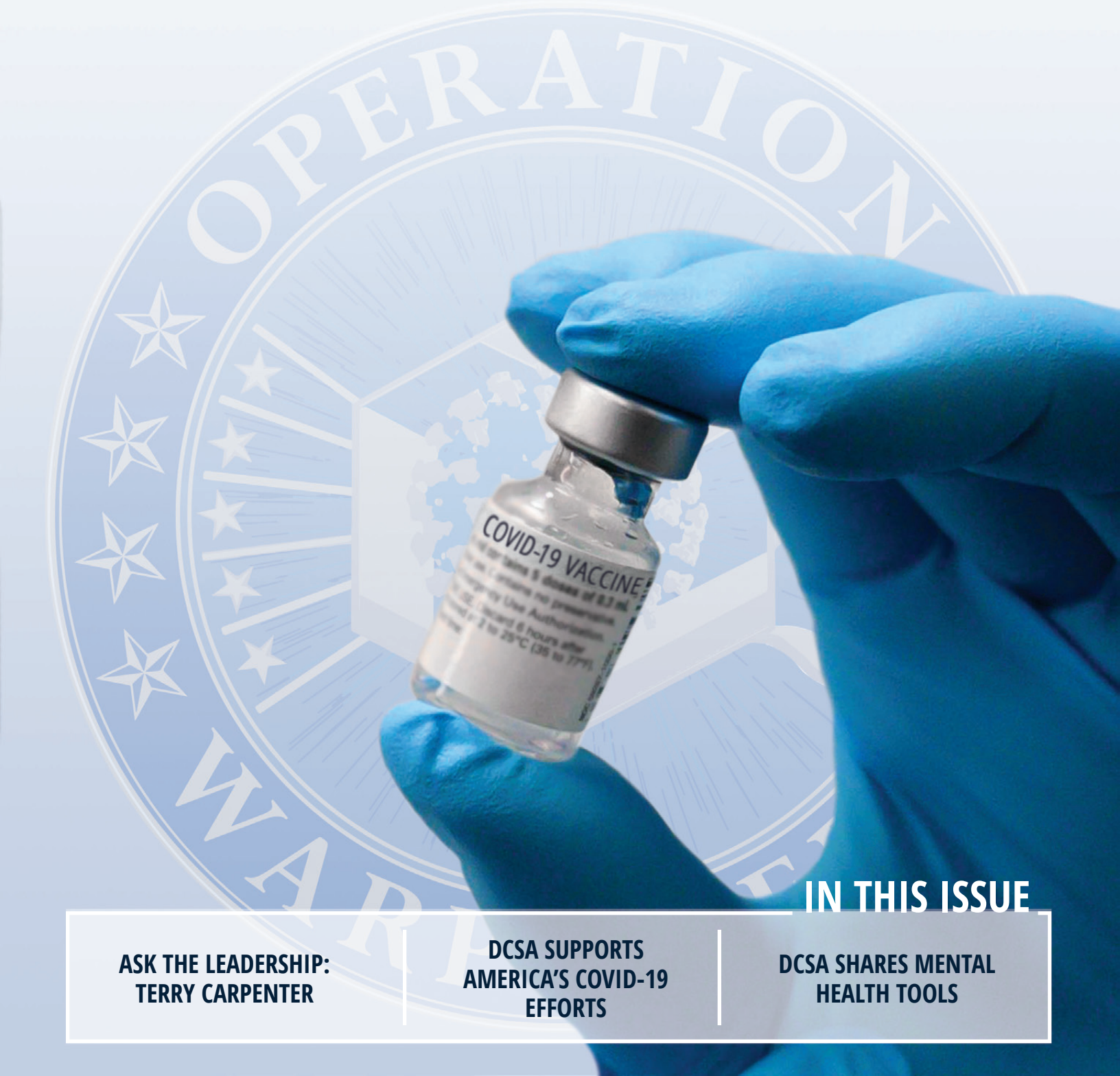
Official Magazine of the
Defense Counterintelligence and Security Agency

# Gatekeeper

Volume 1, Issue 2




## IN THIS ISSUE

# IN THIS ISSUE




VOL 1 | ISSUE 2

## DCSA Gatekeeper

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

27130 Telegraph Road
Quantico, Virginia, 22134

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

# FROM THE DIRECTOR

Welcome to the second issue of the DCSA Gatekeeper. By the time this issue goes to print, my one-year anniversary with DCSA will have passed. It has been an incredibly busy and challenging first year, but from my perspective, it has also been incredibly rewarding. As I have said before, I came to DCSA not from a security background, but as an outsider focused on transformation and innovation. I didn't know exactly what I would find, but I remain in awe of the dedication and commitment of the DCSA workforce. There is no other job I would rather have, and no team I would rather be a part of.

When I assumed leadership of DCSA, it was shortly after the large scale COVID-19 lockdowns. I took the oath of office in our headquarters conference room with fewer than 10 people in attendance and no handshaking. Little did we know how routine the COVID-19 protocols would become and how long they would remain in place. But even more notable is the exceptional performance of this agency during both a pandemic and a major transition.

Our cover article features DCSA's industrial security and counterintelligence support to Operation Warp Speed (OWS). OWS is one of the most significant development and distribution projects the federal government has ever undertaken. The need for COVID-19 vaccines is absolutely critical to being able to return to some sense of normalcy in the United States and around the world. I have often said DCSA employees are in unique positions in that their jobs can have a direct impact on national security. Our support to OWS is yet another demonstration of that. It was cross-functional, involving multiple offices and local field offices. Besides providing vital support to the OWS mission and bringing COVID-19 under control, this experience will serve us well in a new, integrated Operating Model. I applaud the DCSA employees who supported this critical effort and quickly adapted their knowledge and skills to the new challenges of a pandemic.

I also want to highlight the "Ask the Leadership" interview with Terry Carpenter, DCSA's Program Executive Officer (PEO). Terry and his staff transferred to us from the Defense Information Systems Agency (DISA) on October 1, 2020. The PEO model is new to DCSA, and it is important to understand the PEO's role in the agency and the larger acquisition process. With the PEO, DCSA also assumed responsibility for the National Background Investigation Services (NBIS). NBIS is another example of the direct impact DCSA employees have on national security. When fully deployed, NBIS will touch nearly every vetted individual supporting the federal government and industry. It is a huge undertaking and immense challenge for DCSA, but one on which I am confident we can deliver.

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

William K. Lietzau

Director,
Defense Counterintelligence
and Security Agency

# ASK THE LEADERSHIP

## TERRY CARPENTER

### Program Executive Officer (PEO)

***Editor's note:*** *In each issue of the Gatekeeper we feature an interview with a senior leader on their background, mission and program and priorities. Terry Carpenter formally joined DCSA in October of 2020 with the transfer of the mission from the Defense Information Systems Agency.*

Terry Carpenter, the Program Executive Officer (PEO) for DCSA, is responsible for the direction and synchronization of multiple portfolios of information technology (IT) systems that support both federal and defense services for DCSA operations. In this capacity, Mr. Carpenter is responsible for the cost, schedule, and performance of these IT systems.

Prior to his current role, Mr. Carpenter served as DISA's PEO for Services Development, where he was responsible for the acquisition of enterprise and warfighting IT services. He provided acquisition oversight for multiple portfolios of joint programs that deliver enterprise services and data systems for DISA's business operations, its Department of Defense (DOD) collaboration, global cloud computing services, and warfighting command and control services, earning the Secretary of Defense Exceptional Civilian Service Award. Previously, he served as the chief of the Requirements and Analysis Office, where he established a new office that analyzed and maintained the requirements baseline and developed business cases for investments in new capabilities aligned with DISA and DOD strategic guidance. He was also the technical director for the DISA Component Acquisition Executive (CAE). There, he led the development of acquisition strategy and technical implementation, which included four major portfolios covering enterprise services, cybersecurity, command and control, and telecommunications.

### Q: Tell us about yourself and your background?

**A:** I consider myself fortunate to have had great opportunities at the right time in my career, as well as some tremendous mentors. I started public service in the U.S. Coast Guard in the Aids to Navigation (ATON) business. I spent four years at sea, built a new class of buoy tender, and spent several years as a reservist search and rescue controller.

I left active duty to study artificial intelligence and natural language processing, as well as to follow my passion for computers. My most rewarding experience was as a research assistant, where I worked with a young man who could only communicate with a push-button, icon-based speech device. He opened my eyes to the power of technology. Something as simple as email connected to his device changed his life and mine.

Over the next decade, I helped large Fortune 500 and innovative startup companies. I learned to appreciate the ability of people coming together to make it work when the "book" answer doesn't always apply.

While working with the Navy Enterprise Resource Planning (ERP) program as the technical director, I learned to lead a team of more than 500 people,

developing, deploying, and operating one the largest financial and supply SAP ERP systems in the world. It was amazing to be a part of this delicate dance of so many teams representing such a wide variety of skills to achieve a technical solution many thought would fail.

At DISA, I led technology alignment of all acquisition programs across six PEOs for the Component Acquisition Executive, established a new office to develop business cases for new agency requirements, and led a PEO for enterprise services and warfighting systems. That led me to NBIS and a transfer to DCSA as the PEO. All of this infused me with a passion for finding the balance in acquisition best practices and innovation agility.

## Q: What is the role of the PEO in DCSA?

**A:** The PEO balances risk, cost, schedule, performance, interoperability, sustainability, and affordability of a portfolio of acquisition programs. They ensure the portfolio delivers an integrated suite of mission effective capabilities to missions and users. That is a simple statement for a very challenging process. The PEO works closely with the agency CAE, Director Lietzau, and the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) to provide executive oversight of programs, while continually adjusting to the realities of the day. This also requires a close relationship with the sponsor (source of funds), mission requirements owner (user community), and innovations across the industry base. IT capabilities are evolving at speeds we never thought possible, and the PEO is the conduit for information sharing across PEOs in other DOD components.

While the CAE is typically the decision authority (DA) for large acquisition programs, others are delegated to the lowest level possible, either the PEO or program manager, depending on the size of the program. The DA specifies the decision points and procedures for assigned programs and will also tailor program strategies and oversight, phase content, the timing and scope of decision reviews, and decision levels based on the characteristics of the capability being acquired (including complexity, risk, and urgency). This does not mean the DA does this alone. DAs know the best decisions are made with all the stakeholders. As the DCSA PEO matures, you will see more regularly scheduled acquisition reviews, including Acquisition Review Boards (ARBs), Quarterly Program Reviews (QPRs), and Interim Progress Reviews (IPRs).

## Q: NBIS is the biggest program you are working, what is it? What should people know about NBIS?

**A:** NBIS was established in 2016 as a program of record to replace BIES, formerly the Office of Personnel Management Background Investigation Enterprise Services — the security clearance background investigation system that had fallen victim to the single largest data exfiltration in history.

NBIS started with acquisition planning and program standup in September 2016. In 2018, the program made a strategic shift to move development to the cloud and awarded one of the first and largest Other Transaction Authority (OTA) contracts at DISA. Today, the PMO is incrementally delivering systems that are collectively creating a government-operated software-as-a-service (SaaS) for the whole of government, including federal agencies, DOD, and cleared industry. NBIS is responding to and driving transformation in accordance with the new national-level vetting standards defined in Trusted Workforce 2.0 policies.

Beyond the capabilities required to enable the background investigation mission, the NBIS team is concurrently developing and delivering innovative capabilities that enable the transformation of related personnel vetting mission functions. These functions include the adjudication of clearances, continuous vetting of cleared individuals, and screening of multiple categories of foreign nationals seeking to study and/or work with the federal government.

DCSA is leveraging NBIS investments in security, tools, Agile program best practices, code development, automation of operationalization procedures, and advanced analytic capabilities. These investments are dramatically accelerating the PEO's ability to more rapidly support the other missions of DCSA with a proven and secure information platform that enables artificial intelligence capabilities, saving taxpayer dollars.

## Q: What are the biggest challenges you see for the PEO?

**A:** We have tremendous challenges before us. Some of the biggest challenges are organizing, staffing, and instituting the "Big A" acquisition business process and practices, while at the same time managing several complex IT systems at various stages of their lifecycle.

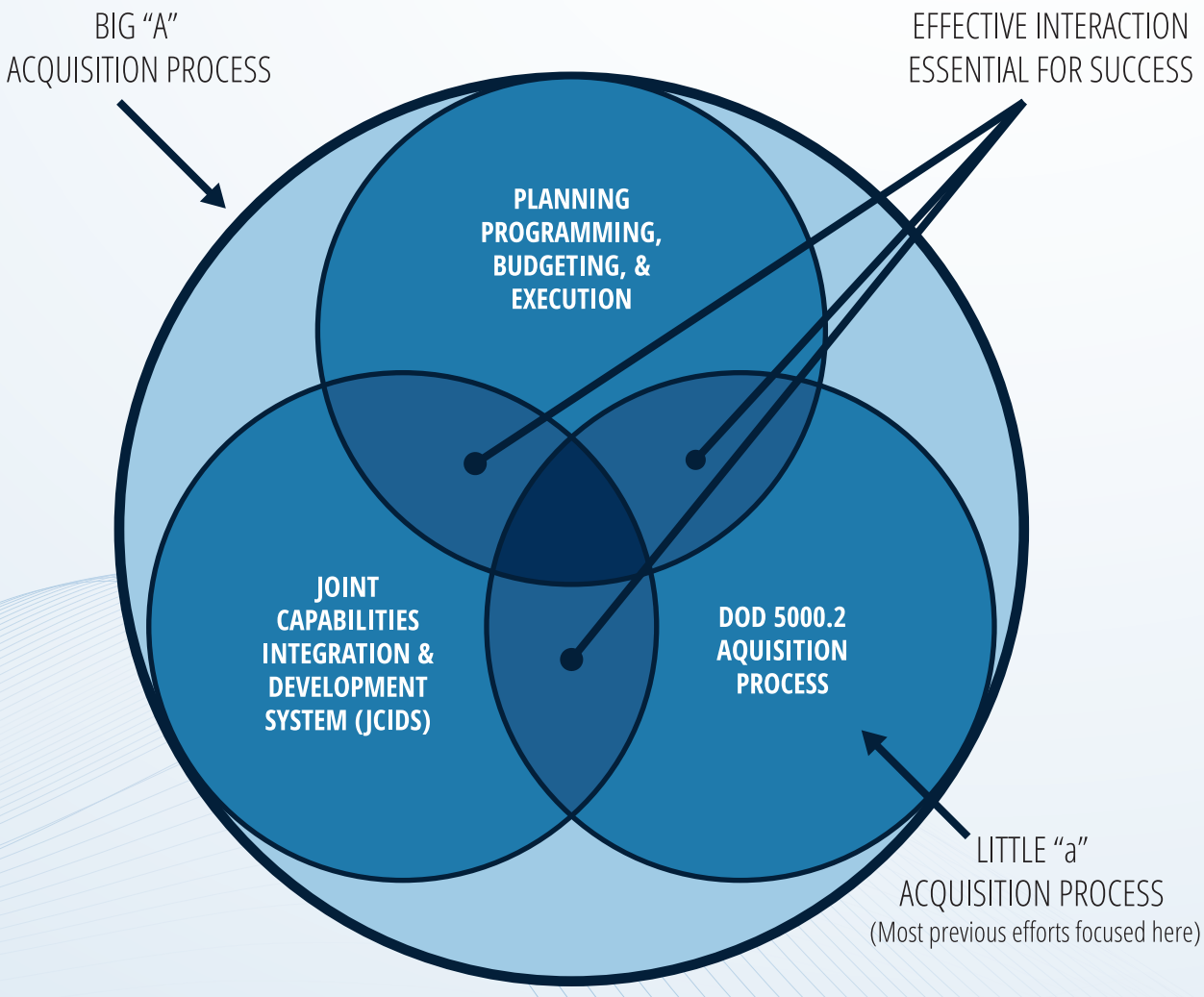
I have to say, perhaps the most important challenge is educating the agency on our PEO role and instilling trust. Even though PEOs are an institutional construct across DOD, organizationally, we are a new function within DCSA. Some people in the agency may not be familiar with a PEO, or what they really do, which can lead to skepticism and apprehension. No one wants to give up control of their fate and put it in the hands of this unknown entity, but that's what PEOs do every day across DOD. We're here to prove we can make a difference for each DCSA mission.

## Q: What do you do mean when you say "Big A" acquisition?

**A:** That's a great question, because the use of the term "Big A" acquisition varies and is not well understood by people outside of the acquisition community.

"Big A" acquisition refers to the common understanding of a highly complex, interconnected acquisition process that is governed by a cross-section of DOD policies and statutory law, cutting across requirements, funding, contracting, and acquisition. However, "Little a" acquisi-

## THE ACQUISITION SYSTEM



tion refers to basic acquisition program management and contracting. There is a distinct difference between the complexity of developing a contracting strategy for a major acquisition program ("Big A") and establishing contracts for commercial off-the-shelf products and services ("Little a"). Establishing contracts for "Big A" acquisition accounts for the various intricacies across the defense acquisition system phases, or cycles, which involve research, engineering, development, production, testing, delivery, training, operations, sustainment, and disposal. It's even more dynamic with contracts for software development for IT systems. CAEs and PEOs must manage this complexity of the "Big A" acquisition system through active oversight and strong partnerships with the requirements, financial, and system development processes. That's why stakeholders from each of these functions are seated at the table for any acquisition decision or review.

## Q: What are the biggest opportunities you see for the PEO?

**A:** Our biggest opportunities are to hire fresh minds and bring in new perspectives to the PEO. Another is the ability to leverage recent reforms directed by Congress to incorporate the latest technologies, such as cloud-based platforms, and industry best practices, such as Agile and Lean methodologies, as well as development, security, and operations (DevSecOps) software factory. These new ways of doing business being used for NBIS fully engage the mission owners in the development of capabilities throughout the lifecycle to incrementally develop and get capabilities into the hands of the user at the "speed of relevance." By implementing systems in secure cloud-computing environments, our programs are more efficient and effective than making capital investments in an agency-built and owned infrastructure.

## Q: Is there anything else you would like the workforce or external stakeholders to know about the PEO?

**A:** We live in a sophisticated world with complex challenges that we are working hard to more fully understand and address. The challenges include a barrage of foreign and domestic individuals, groups, and nation-states, all seeking to impact the health and safety of the United States and its citizens for personal or collective financial, ideological, or political advantages. They are using ever more advanced means to mask, hide, or obscure their actions and intent within the digital overload of traffic on the internet today.

The PEO is employing best-of-breed cyber tools and methods through every stage of capability development to stay ahead of the attacks that would steal or alter DCSA's data. At the same time, we are working to construct artificial intelligence capabilities in new and unique ways, enabling DCSA's missions to rapidly sift through and make sense of mountains of data in ever more efficient and effective ways.


# DCSA SUPPORTS THE NATION'S COVID-19 EFFORTS THROUGH OPERATION WARP SPEED

**By Beth Alber**
Office of Communications and Congressional Affairs

In early 2020, the federal government sought to aid the development and distribution of a vaccine to counter the rapidly spreading COVID-19. Congress provided almost $10 billion in funding, and in April 2020, the U.S. government established the public-private partnership known as Operation Warp Speed (OWS).

OWS employed a whole-of-America approach, led by the Department of Health and Human Services (HHS) and the Department of Defense (DOD). Serving as part of the Federal COVID-19 Response (FCR), the OWS leverages the expertise of HHS scientists, DOD planning and logistics capability, American industrial ingenuity, and academic innovation.

DCSA has played a critical support role, providing direct industrial security assistance on the Security & Assurance (S&A) team, counterintelligence (CI) support through the analysis cell, and an interagency partnership with the FBI's National Counterintelligence Task Force (NCITF). Approximately 67 DCSA employees from Critical Technology Protection (CTP) and CI provided their expertise and supported OWS in some capacity.

"We've got several employees supporting Operation Warp Speed. The DCSA team, to a significant extent, was protecting the development of vaccines as part of OWS," said DCSA Director William K. Lietzau during a recent agency town hall, noting the speed in which the vaccines were created. "[It] has been an amazing accomplishment for the United States."

## INDUSTRIAL SECURITY SUPPORT

CTP personnel began supporting OWS in June 2020 when two individuals — Senior Industrial Security Representative (ISR) Ann Marie Smith from the San Francisco Field Office and ISR Larissa Caton from the Hanover 2 Field Office — were detailed to the OWS Security and Assistance (OWS S&A) directorate, located in the HHS building in Washington, DC.

"The high speed of producing multiple safe and effective vaccines in about one-fifth of the standard time frame — and also distributing millions of doses each week — creates a dynamic security challenge requiring a depth of professional knowledge, accelerated critical thinking, and strong skills in collegiality with constant humility," said Smith.

According to Smith, the team started by fashioning a security model to evaluate risk to the overall operation, mapping the supply chains, and developing an evaluation model for assessing risk at contractor facilities involved in vaccine production.

"When our team was first handed this mission, it was nebulous, vague, and most often, confusing. It was the very definition of building the plane while flying it," said Caton. "Through constant teamwork and coordination, the FCR S&A team simultaneously created a new model for evaluating security risk tailored to the biopharma industry, while also identifying the critical facilities in the supply chain responsible for bringing these vaccines to life.

"Leveraging our institutional knowledge and, when appropriate DCSA CI support elements, we were able to track and evaluate threat and vulnerability to key vaccine participants to effectively mitigate the greatest levels of risk," Caton continued. "A key part of this was developing personal relationships with facility security personnel, where our roles as industrial security representatives were useful when engaging with industry."


Ann Marie Smith, otherwise a senior ISR within DCSA's San Francisco Field Office, began serving at Operation Warp Speed in June.

Once the model was created, DCSA identified industrial security specialists to assess OWS contractor risk. Approximately 60 volunteers in the CTP workforce were then educated on the basics of the Federal COVID-19 Response, vaccine production process, and evaluation approach.

## COUNTERINTELLIGENCE SUPPORT

CI support to the FBI NCITF interagency partnership started in May 2020 and involved approximately 70 CI special agents, analysts, cyber analysts, targeting analysts, and collection managers across the nation, providing support at cleared and uncleared companies. Additionally, CI employees were strategically placed at key government sites.

DCSA's CI strategy — developed without key data normally available to support a traditional CI approach — focused on identifying and mitigating threat across the supply chain and using analysis to uncover threat throughout the biotechnology

and biopharmaceutical ecosystems. To do this, DCSA established desk officers who reviewed and assessed reporting that might impact OWS, then used that information to identify and assess threats to other areas. The desk officers requested analysts generate finished threat intelligence on OWS suppliers that were deemed most at risk of foreign intelligence entity exploitation and then forwarded the intelligence to other government agencies (OGAs) for investigative or operational action.

CI also took a top-down approach, working with other CI agencies to identify technologies and processes critical to the biopharma ecosystem. This resulted in the development of the Biopharma Terminology Framework (BTF), a list of more than 1,100 terms and processes that are unique to the development of critical therapeutics, vaccines, and diagnostics. The CI team used the BTF for specific activities supporting the protection of OWS efforts.

DCSA CI also developed "fly-away" packages to use while conducting outreach at OWS-affiliated contractors. The packages included critical information that enabled a CI agent to engage an OWS contractor, determine the extent of the contractor's involvement in OWS, collect information vital to the U.S. government, identify and mitigate threats directed against the contractor, and establish a line of communication for reporting of future suspicious activities.

Air Force Senior Airman Domingo Rodriguez, an aerospace medical technician with the Puerto Rico Air National Guard, administers COVID-19 vaccines in Carolina, Puerto Rico, Feb. 16, 2021. Airmen are helping to vaccinate residents of Puerto Rico at mass vaccination distribution sites.

In conjunction with FCR S&A, CI hosted an OWS-themed webinar, focusing on threats to pharmaceutical and biotechnology sectors as well as industrial security best practices. It reached more than 1,300 participants from uncleared and cleared companies across the nation as well as state, local, and federal government entities. Highlighting the importance of CI in these sectors, the first webinar's keynote speaker was delivered by William Evanina, former director of the National Counterintelligence and Security Center (NCSC).

## TRAINING SUPPORT

At the request of FCR S&A, the Center for Development of Security Excellence (CDSE) created an "Operation Warp Speed and Beyond" toolkit for predominantly uncleared OWS companies. In less than 45 days, CDSE published the toolkit and hosted it on their website. The toolkit contains more than 200 resources for insider risk, CI awareness, industrial security, risk management, information security, operations security, cybersecurity, personnel security, and physical security.

The toolkit also included several new CDSE products, such as an original OWS poster dispatched to eight OWS industry partners and HHS as well as a webinar on "Counterintelligence and Insider Threat in a Time of COVID-19."

CDSE coordinated with the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), and HHS to develop and distribute an "Insider Threat Implementation Guide for Healthcare and Public Health Sector" job aid to OWS partners. The job aid supported the development of insider threat risk programs within those critical sectors.

An Air Force airman assigned to the 108th Wing, New Jersey Air National Guard, checks the name of a staff member at the New Jersey Veterans Memorial Home at Vineland during COVID-19 RT-PCR testing in Vineland, N.J., Dec. 1, 2020. The test detects the live active virus for SARS-CoV-2, the virus that causes COVID-19.

## FIELD SUPPORT

As of January, CTP personnel had provided security advice, assistance, and assessment to 17 facilities, including all five of the U.S. production facilities for needles and syringes, which comprise about 20% of the supply needed. All five facilities were involved in at least one vaccine's supply chain production, from raw materials to final drug production, including a vial producer, cold storage facility, and more.

"Both facilities I visited primarily focused only on physical security. Neither had a stand-alone security program or dedicated security staff, and neither had a CI or insider threat program," said Senior Industrial Security Specialist Duane Shannon, Tacoma Resident Office. "I found it very easy to take the concepts of the National Industrial Security Program (NISP) and our methodologies and apply them to the unclassified environment in which they were working. For example, as the company and I worked through the business flow, we quickly identified vulnerabilities related to the generators in that they were not being physically protected and, therefore, were vulnerable to sabotage. It was during that discussion that I felt the company started to appreciate and understand the risk, and that was a great feeling. Overall, it was a great experience, and it was an honor to be part of the OWS mission."

The opportunity to bring a lens of threat awareness and security education to a biopharmaceutical partner involved in the development of the COVID-19 vaccine was incredibly rewarding, according to Senior Industrial Security Specialist April Rodriguez-Plott from the Cypress Field Office. "DCSA's security expertise brought insight and a risk-based approach as we discussed the facility operations. The company used the opportunity to reassess their posture and readiness to protect their facility, people, and information from a security lens. The company's leadership team referred to the site visit as an 'eye-opening experience,' which provided many countermeasures to consider to better protect their organization," she said.

"Working on the OWS mission has been the most satisfying assignment thus far in my DCSA career. This mission is such a great example of the whole-of-government approach that our nation has deployed in times of national crisis," commented Senior ISR Ehren Thompson, San Diego Field Office. "It's an opportunity to leverage my professional experience in security, and for my work to impact everyone in the nation in a real way is humbling."

Senior Industrial Security Specialist Mery Neal, San Antonio Field Office, assisted a company that was producing syringes to administer COVID-19 vaccines. "They had very minimal, and in some cases, no security procedures to protect their technologies and assets. DCSA helped the contractor understand the threat to their technology, and they were able to identify gaps in their processes and procedures. As a result, the contractor established an insider threat program and incorporated security in all aspects of their processes and procedures to ensure full integrity of their products and safeguard of their technology. I was grateful and privileged to be able to contribute to this critical mission for our nation," she said.

## DISTRIBUTION SUPPORT

The FCR S&A holds weekly board meetings to review significant prime contractor progress and identify additional resources needed to mitigate risk to operations.

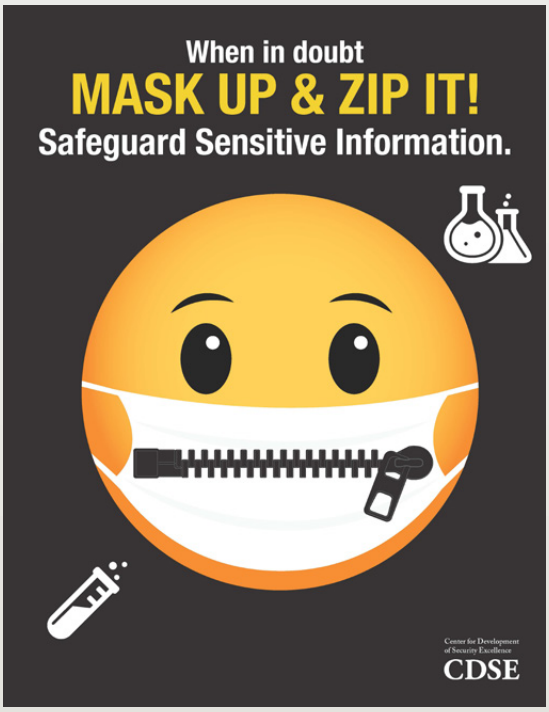
"We continuously adjust supply chain maps according to prime contractors' decisions and identify federal assistance for common concerns," Smith said. "I participate in these boards, brief on findings from DCSA and other assessment visits, identify additional areas of risk, and conduct follow-up actions as assigned."

In December, CTP efforts began focusing on transportation security for vaccine distribution. Smith was assigned to coordinate with the U.S. Marshal Service to support shipments, collect shipment data from all the vaccine companies, and tailor their efforts according to shipment criticality.

"I was tasked with mapping and keeping record of cold storage facilities that would house the vaccine before it was even approved by the Food and Drug Administration (FDA)," Caton said. "I have answered numerous cold storage questions and have helped several interagency partners assess and map potential resource shortages and weak points. Everyone working on this effort is focused on the same goal — getting the American people vaccinated and moving back to a normal life."

"Every week, serving on the FCR team is a personal, professional, and exceptionally fulfilling challenge. I am deeply grateful for DCSA's support of my detail to this highly important national security mission," Smith said. "Army General [Gus] Perna, OWS chief operating officer, stated early in the operation, 'If you are not personally and professionally uncomfortable doing this mission, you're probably not contributing.' That quote propels me through many days and provides me hope that I'm making a difference in our national response against COVID-19."


Larissa Caton, an ISR based out of the Hanover 2 Field Office, offers hands-on support for Operation Warp Speed on behalf of DCSA



# BI FIELD OPERATIONS TURNS TO TECHNOLOGY IN RESPONSE TO COVID RESTRICTIONS

**By Jeff Smith**
**Background Investigations Field Operations**

In March 2020, as the health implications of COVID-19 were recognized as a global pandemic, DCSA's Background Investigations (BI) Field Operations moved swiftly to keep its mission fully functioning, providing security, suitability, and credentialing investigations across the whole of government. At that time, DCSA had dozens of investigators stationed at DOD installations around the globe. As these investigators were being recalled to their contiguous United States duty stations, plans were already taking shape to continue providing DOD and other government agencies with timely, quality investigations both in the United States and abroad, despite the limitations brought on by the pandemic.

Before the pandemic, BI Field Operations had previously piloted alternate methodologies, such as using video interviewing (VI) platforms to conduct certain types of interviews, as permitted by the Security, Suitability, and Credentialing Executive Agents (EAs). The EAs issued approval of broader use of alternative investigative methods based on an exception in the Federal Investigative Standards (FIS) that allows for such use under "rare and exigent circumstances."

BI Field Operations realized the need to ramp up these tools to enable its mission under COVID-19 restrictions. The staff quickly trained on the new VI platforms and educated its customer base on the implementation of the alternate investigative methods. This was no easy task as the primary investigative method has always been in-person interviews with subjects, sources, and record providers, which the team still highly valued.

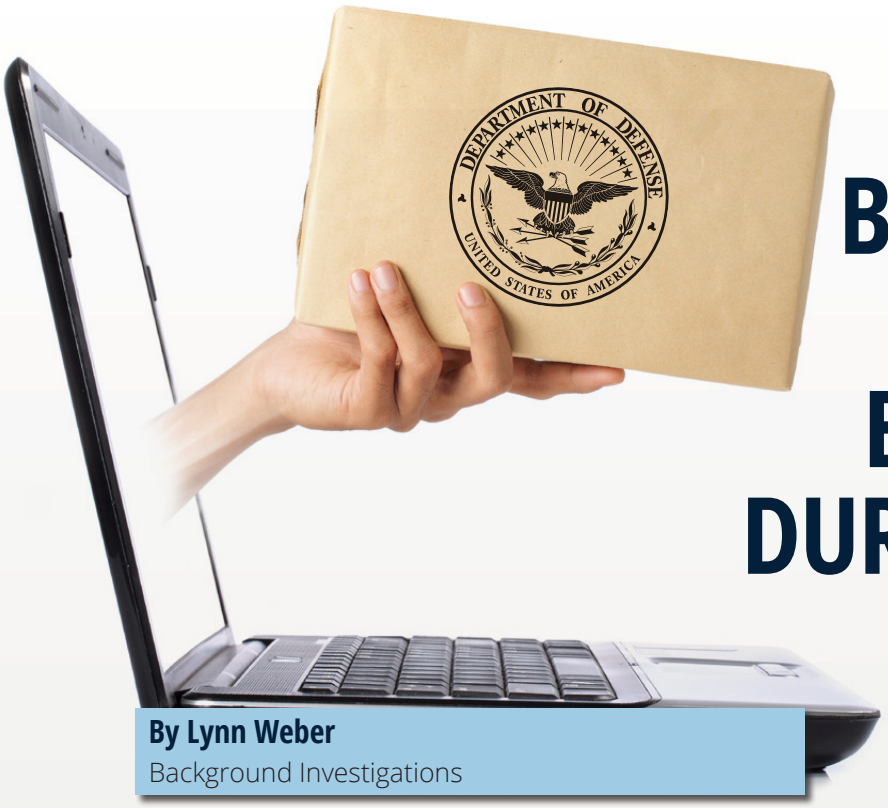
Increasing virtual capacity required collaboration and effort across multiple offices within BI and greater DCSA. BI Field Operations immediately sought DCSA's Office of the Chief Information Officer's (OCIO) assistance to rapidly expand its VI capability. Simultaneously, DCSA's BI Policy and Procedures team began issuing new guidance to the workforce on implementing these new investigative methods.

VI training and support teams were quickly assembled across BI Field Operations, and the process of training approximately 1,600 federal investigators on various communication platforms began in earnest. Not only did the federal field staff have to quickly master the technology, but they also had to learn how to adapt their interviewing techniques to account for the new and increased virtual office setting, all while ensuring and upholding the quality of the investigations.

The BI Field Operations staff is no stranger to change. As daunting as the task was, they rose to the occasion and have so far delivered approximately 63,000 essential subject interviews to adjudicators for eligibility determinations. In fact, some of the individuals under investigation were directly involved in COVID vaccine development and implementation. At the same time, less than 6% of investigations received during the pandemic have been held for in-person completion at a later date.

> ***"While 2020 will be remembered as a year full of unique challenges, it should also be remembered for DCSA's collective ability to overcome unprecedented obstacles."***

Investigators, investigative assistants, and special agents-in-charge all across BI Field Operations demonstrated their commitment to this "no-fail" mission with passion, dedication, and resourcefulness. DCSA's military, government, and industry partners depend on BI Field Operations to conduct and deliver the highest quality investigations in a timely manner. Our national security interests depend on it, even in and especially during a worldwide pandemic.




# BI CUSTOMER & STAKEHOLDER ENGAGEMENTS DURING COVID-19 RESTRICTIONS

**By Lynn Weber**
Background Investigations

As many federal agencies were transitioning to full-time telework to mitigate the risk of COVID-19 last March, DCSA was working large process shifts to support not only the increased telework status but also its ability to continue processing background investigations.

DCSA Background Investigations (BI) needed to address the absence of in-person interactions and support customers who were not in the office to receive hardcopy investigative results, mail, collect fingerprints, or answer phone calls. BI's Customer & Stakeholder Engagements (CSE) agency liaisons served as a coordination and communication hub to DCSA's customers, while the BI Operations divisions changed their processes — from top to bottom in some instances — to accommodate the federal government's "new normal."

CSE is the gateway to the BI mission for more than 140 federal agency customers, state, local and tribal law enforcement agencies, applicants, and other stakeholders. CSE is comprised of a team of agency and systems liaisons, applicant knowledge center representatives, and law enforcement agency liaisons who provide guidance, subject matter expertise, and other critical information to enable customers and stakeholders to do business with DCSA/BI and to achieve mission success.

Not long after the pandemic began, DCSA's returned mail from customer agencies began to accumulate because customers were not physically in the office to receive it. These mailings included closed case material, which is essential to the adjudications and onboarding process. DCSA immediately developed a system to triage the thousands of pieces of returned mail and worked to develop an interim secure electronic delivery method for each agency. While these modifications allowed DCSA and its customer agencies to telework safely and receive essential communications, it still involved some form of manual processing.

What DCSA still needed was a fully electronic delivery method for the smaller agencies and agencies that relied heavily on hardcopy closed case materials. DCSA worked quickly to expand eDelivery, which automates the delivery of closed investigations through a secure platform. The benefit of eDelivery is that it does not require any manual processing, decreases the time for delivery after closing, and eliminates the need for manual file maintenance. As of January 2021, 57 agencies have transitioned to this new eDelivery method.

Another ongoing challenge DCSA customer agencies have faced during the pandemic has been collecting fingerprints required for onboarding and credential processing. The Office of Personnel Management

(OPM) issued a memorandum allowing investigation processing to continue without fingerprints in situations where they cannot be obtained due to facility closures or other obstacles unique to the current working environment. However, agencies are still required to submit fingerprints for these individuals as soon as they are able in order to meet Federal Investigative Standards (FIS). DCSA CSE agency liaisons continue to work closely with customer agencies to track investigation submissions without fingerprints due to COVID-19 and ensure that fingerprints are submitted as soon as possible.

CSE will continue to communicate all COVID-19 mitigation strategies to its customers during monthly meetings, written communications, posts on the DCSA website, and email correspondence. CSE also coordinates with the Security, Suitability, and Credentialing Executive Agents and other policy makers, including the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), so they can provide timely updates at monthly stakeholder meetings. The latest feedback from customers on DCSA's COVID-19 mitigation strategies was positive:

*"DCSA was very proactive and transparent in helping us adjust to change during COVID-19. DCSA's operational changes were and are still very effective."*

*"Adjusting quickly during the COVID environment has been refreshing. DCSA took reasonable and practical steps to ensure the work could continue, and I really appreciated that."*

These comments capture the dedication and effort not only of CSE but each and every DCSA office working to ensure the BI mission remained effective during the COVID-19 pandemic.

## CUSTOMER ADVISORY BOARD

One of the ways that CSE is engaging with its stakeholders is through a series of meetings, each with a different focus or audience.

DCSA — through its predecessor agencies — has engaged with its stakeholders since 2009 via a variety of stakeholder meetings. After the October 2019 transfer, DCSA decided that the quarterly Customer Advisory Board (CAB) was the appropriate venue to merge its communications to customers for a collective voice as an agency. For this to happen, the new CAB meetings had to cover all mission areas within DCSA including personnel vetting, industrial security, counterintelligence support, and training. A DCSA working group with points of contact from each DCSA division made what first seemed like a difficult task easier through collaboration, making the impossible possible.

The first introductory CAB was in November 2020, with two virtual sessions — one with federal government agencies and the other with industry representatives. During these meetings, DCSA leadership introduced the organization's newly merged structure and provided updates on topics, including information technology system developments, Continuous Evaluation (CE), and training. Despite being held virtually, participation was significant. CAB membership is limited to federal agencies and industry partners that submit large volumes of investigations, hold large numbers of cleared facilities, or represent large industrial organizations. Future meetings are intended to allow senior executives from across the federal government and industry to collaborate and partner with the DCSA director and senior leadership in a way that furthers DCSA's effectiveness at conducting its missions.

## BACKGROUND INVESTIGATIONS STAKEHOLDERS GROUP

The Background Investigations Stakeholders Group (BISG) is one of — if not the — most significant engagement venues for consumers of DCSA's BI services. For more than a decade, the BISG has come together on the third Thursday of each month to discuss all things related to background investigations. Presentations focus on policy, systems, processes, and procedures with special presenters from across the mission space, including the FBI, Office of the Director of National Intelligence (ODNI), OUSD(I&S), OPM, and more. Headquarter-level representation from BI customer agencies (typically within their personnel security and human resources offices) are invited from across government. Attendance is usually around 200-300 individuals. With the transition to DCSA, the BISG has broadened its scope of presenters to include new investigations-focused divisions within DCSA such as the Vetting Risk Operations Center (VROC) and the Program Executive Office (PEO).

# PERFORMING BACKGROUND INVESTIGATIONS IN TWO LANGUAGES

**By Background Investigations Puerto Rico Field Office**

The following BI Special Agents contributed to this article: Chrystal Calendar, Darlye Coronado, Angel Landrau, Christian Mendez, and Stacy Torrado

*Did you know that Spanish is the only official and primary language of Puerto Rico?*

Spanish is the dominant language of business, education, and daily life on the island of Puerto Rico, spoken by nearly 95% of the population. In addition to conducting high-quality investigations, DCSA's Puerto Rico-based BI special agents face a location-specific challenge: They must perform investigations in both English and Spanish.

For agents working in Puerto Rico, translating and interpreting from Spanish to English can be both brain-intensive and time-consuming. When positions for Puerto Rico are advertised, bilingual proficiency is a requirement. An agent's ability to communicate and translate between Spanish and English is confirmed during the hiring process and continues to be monitored and validated during a rigorous training process, which can take up to a year or more. On the job, the agents practice simultaneous interpretation, translation, and sight translations daily.

During an investigation, subjects, sources, and record providers typically request interviews be conducted in Spanish. Agents must therefore conduct the interview in Spanish but take

notes in English (e.g., simultaneous interpretation). It's important that the information is correctly and precisely interpreted. Most police, medical, employment, education, and court records are also in Spanish and need to be translated. Additionally, subjects typically don't understand the contents of agency releases written in English so agents must read the forms aloud to the subjects in Spanish to ensure comprehension.

Agents in Puerto Rico have found that conducting interviews in Spanish elicits the most accurate and thorough information. It makes a reluctant interviewee feel comfortable, confident, and relaxed, while trying to provide all the complex information that is being sought for a background investigation. Agents will typically also add Spanish voicemail recordings to their government cell phone to ensure responses from subjects, sources, and record providers.

Due to the complexity of legal terms, police and court records checks are some of the most arduous translations that agents perform. While taking notes from the records, there are times when a specific legal term is too complex to translate immediately. The agent will write the Spanish word in their notes then later research the exact English meaning. An inaccurate translation can lead to serious consequences, potentially impacting the outcome of an investigation. Unfortunately, when translating from Spanish to English, there are many words that may appear the same, but have multiple meanings.

When typing the report of investigation (ROI) — the final output of an investigation — it can be a challenge to avoid misinterpretations, errors, and inconsistencies. The ROI must be in English for the adjudicator to make an appropriate security or suitability determination. Therefore, it is vital that all translations use the correct terms to avoid impacting the background investigation.

DCSA's Puerto Rico agents also use their bilingual capabilities to support the larger BI mission. They assist other divisions by performing translation duties, such as translating Spanish-language inquiry letters written and conducting interviews in Spanish for special investigations.

Although a laborious task, bilingual agents in Puerto Rico execute and meet mission goals. Performing investigations in two languages is a routine part of the work, and it is carried out every day with the utmost professionalism and integrity.

# SUITABILITY, FITNESS, AND CREDENTIALING ADJUDICATIONS

## DEDICATED GROUP OF PERSONNEL SECURITY SPECIALISTS ADJUDICATES 42,000 INVESTIGATIONS ANNUALLY

**By Nadia Bebawy**
DOD Consolidated Adjudications Facility (CAF)

DCSA's CAF is the sole authority determining security clearance eligibility of non-Intelligence agency, DOD personnel occupying sensitive positions, and/or requiring access to classified material. This includes suitability, fitness, Homeland Security Presidential Directive 12 (HSPD-12) credentialing, and child care cases.

A specialized group of 34 DCSA personnel security specialists adjudicates, on average, more than 3,500 suitability, fitness, and credentialing background investigations each month. The DOD CAF established this dedicated group of personnel security specialists solely for these complex and diverse investigations. Each adjudicative determination serves a different purpose and relies on unique adjudicative criteria.

**National Security Determinations** apply to civilian, military, and contract personnel who are assigned to positions requiring access to classified national security positions. Whereas, national security determinations use the 13 adjudicative guidelines to determine whether employment would constitute a risk to national security and related activities that require use of, or access to, classified information including positions, facilities, and systems. In short, national security determinations determine the trustworthiness for access to classified information. As the criteria are applied, it is possible for an individual to be found suitable or fit for employment, but ineligible for a security clearance, or vice versa.

**Suitability Determinations** apply to federal employees and are based on the "position designation risk levels" — low, moderate, or high — of the position duties required. The suitability determination reviews an individual's character traits and conduct to determine whether the individual is likely able to carry out the duties of the position with integrity. Suitability determinations apply eight standard guidelines to the individual's past and current actions to determine if their character and conduct will promote the efficiency and protect the integrity of the service.

**Fitness Determinations** use the same eight guidelines as for suitability to determine whether a person's character, in this case a contract employee, is acceptable to perform duties on behalf of a federal agency. In short, suitability and fitness determinations assess if an applicant is suitable for employment.

**HSPD-12 Credentialing Decisions** ensure an employee does not pose a risk to life, safety, or health of people, assets, or information. HSPD-12 sets a policy for common identification standards for secure and reliable forms of identification for federal employees and contractors requiring long-term access to U.S. government facilities and information technology systems. The HSPD-12 directive specifies six basic adjudicative guidelines and seven supplemental adjudicative factors. In short, HSPD-12 determines and standardizes Common Access Card (CAC) identifications.

In addition, the CAF team also considers background investigations within the **DOD Child Care program**. These background investigations, frequently referred to as "child care cases," are reviewed to protect children by denying or removing any applicant, current employee, contractor, or volunteer, who is unsuitable to provide child care services due to derogatory information contained in their background investigation. Child care cases use a unique set of guidelines separate from the HSPD-12, suitability, or national security criteria.

Given the variable factors of each background investigation, these adjudicators maintain the Adjudicator Professional Certification (APC) and Due Process Adjudicator Professional Credential (DPAPC), as well as completing additional in-depth training related to HSPD-12, suitability, fitness, and DOD Child Care program guidelines. The complexity of each program along with the training requirements and the need for attention to detail make these personnel security specialists among the most well-rounded and highly skilled adjudicators at the DOD CAF.

# USING THE BEST TOOLS TO MANAGE STRESS CAN MAKE A HUGE DIFFERENCE IN YOUR OVERALL WELLBEING

**By Michael Priester, Chief Psychologist, and Elisabeth Jean-Jacques, Psychologist**
DOD Consolidated Adjudications Facility

**Editor's Note:** *May is Mental Health Month, and this year's theme set by Mental Health America is "Tools 2 Thrive." This article is intended to offer coping mechanisms for anyone suffering from stress.*

Though many of us routinely face stressful challenges in our lives, the past year has presented extraordinary challenges. We have experienced an unrelenting pandemic, which has sorely limited our opportunities to work, socialize, exercise, and otherwise engage in our favorite activities. We have witnessed events that illustrate our country's social inequalities and prejudices. We have seen large numbers of people begin to outwardly distrust previously trusted core societal institutions and processes, due in part to misinformation campaigns. And finally, for DCSA personnel in particular, we have continued to integrate into a new agency, which has resulted in changes to organizational expectations and, in many cases, supervisors. While these workplace changes may ultimately result in an overall positive outcome, the process itself can be stressful.

When you consider these mutually shared stressors, as well as the individual stressors that you and your family may have experienced in the past year, having the best tools to manage stress can make a huge difference in our overall well-being. As Dr. Hans Selye, a physician and pioneering stress researcher, has observed: some people are better equipped to cope effectively when faced with challenging circumstances. In fact, some individuals thrive despite the degree of stress in their lives. Why might this be?

> ***"It's not stress that kills us, it's our reaction to it."***
>
> — Dr. Hans Selye, physician and pioneering stress researcher

## WHAT IS PSYCHOLOGICAL STRESS?

Psychological stress happens when an individual perceives a situation is likely to exceed their psychological, social, or physical coping resources or coping strategies. Stressors can be positive or negative events, and they can present problems that are clearly solvable or include aspects that are largely out of a person's control. People vary in their tolerance to stress, as well as their performance in the face of stress. In fact, some individuals show improved performance under stress, and they may even attempt to increase their stress level, such as an athlete trying to psych themselves up before a competition. Feeling stressed or even overwhelmed is not a sign of weakness or poor coping. Everyone feels overwhelmed with life stress from time to time.

## HOW DO PEOPLE COPE EFFECTIVELY WITH STRESSFUL SITUATIONS?

In their 1984 work "Stress, Appraisal, and Coping," psychologists Richard Lazarus and Susan Folkman theorized that all coping strategies could fall within two basic categories: problem-focused and emotion-focused techniques.

Problem-focused coping strategies involve directly solving the issue that is creating the stressful situation. These strategies may include defining the problem, considering courses of action, thinking about the pros and cons of each one, and finally, acting on a course of action. Emotion-focused coping techniques reduce the emotional distress experienced when someone encounters a stressful situation. These strategies may include distraction, talking to someone about your feelings, meditation, mindfulness, prayer, or showing gratitude in one's life.

## WHICH COPING STRATEGIES ARE BETTER — PROBLEM-FOCUSED OR EMOTION-FOCUSED?

Research has shown that those individuals who function most effectively under high stress circumstances are those who use a wide range of both emotion- and problem-focused coping strategies. Many individuals initially try to solve their problems directly as a way of reducing their stress level. This may be the best tactic when the problem is solvable. But remember, many stressors have both solvable and unsolvable components. For example, the COVID-19 pandemic may have impacted your finances, your ability to exercise or engage in good self-care, and your ability to socialize with supportive persons in your life. While employing problem-focused strategies, such as budgeting and finding new sources of recreation are essential, feeling lonely or isolated may not be directly solvable. To cope effectively with overall pandemic effects, a capacity to use emotion-focused strategies is also necessary.

## OTHER ITEMS TO CONSIDER:

- When faced with stressors that have clearly unsolvable components (e.g., receiving a terminal cancer diagnosis), those who attempt to use only problem-focused coping strategies may experience greater anxiety or depression when they are unable to solve the problem.
- General self-care, including regular exercise, sleep, nutrition, and as much social support as possible, should be seen as psychological preventative care. Individuals who practice a regular regimen of good self-care may periodically feel overwhelmed but are better prepared for stressors.
- Several studies have shown that individuals who showed gratitude for things in their life showed improvements in their mental health, even when they were experiencing high levels of stress.
- While avoidance as a coping strategy can have a negative connotation, there is nothing wrong with unplugging from the 24-hour news cycle and social media feeds. In fact, it is essential to good self-care to form good boundaries with the endless onslaught of stressors we have faced over the past year.
- Lastly, it is important to be aware of strategies that may relieve stress in the short term but can worsen stress over time. One recent survey showed that alcohol consumption between March 2019 and March 2020 spiked 54%, which suggests that some people used alcohol as an emotion-focused coping strategy during the pandemic. For many individuals, there may be little harm in the occasional alcoholic beverage. However, the use of alcohol and other mood-altering substances as regular coping methods may lead to adverse long-term consequences.

## WHAT'S THE BOTTOM LINE?

Those who have a more solid repertoire of coping strategies, both emotion and problem-focused, will both feel and perform better when under stress. Good self-care is an important foundation to cope effectively. Be grateful for good things in your life and unplug from endless news and social media feeds for some time each day.

## FOR MORE INFORMATION:

1. Seek support and assistance when you need it through the DCSA Employee Assistance Program by calling 1-866-580-9046. Remember: merely seeking mental health care will not impact your clearance eligibility.
2. Mindfulness and meditation are two excellent emotion-focused coping techniques. There are many excellent books, apps, and even a currently streaming program to help you develop these skills.
3. Read the Harvard Mental Health Letter "In Praise of Gratitude: Expressing thanks may be one of the simplest ways to feel better" for a summary of findings on gratefulness research: https://www.health.harvard.edu/mind-and-mood/in-praise-of-gratitude.
4. CAF mental health FAQs and resources can be found at: www.dcsa.mil/mc/pv/DOD_caf/FAQs/ and www.dcsa.mil/mc/pv/DOD_caf/resources/.

# DCSA USES DATA SCIENCE TO STREAMLINE ADJUDICATIONS

**By Mark Nehmer**
Program Executive Office

In the 16th century, an astronomer observed and recorded the movement of terrestrial bodies for decades. He compiled significant amounts of data but was unable to interpret or use the data in any meaningful way. It took another astronomer and mathematician, Johannes Kepler, who later applied what we would call today data science, to deduce from this old data the first two planetary motion laws. These laws allow us to understand how the planets in our solar system move and accurately predict their location at any given time.

Our information systems collect, process, and generate vast amounts of data from business and private transactions, communications, postings of records, articles, studies, forecasts, video feeds, blogs, sentiments, etc. All these data sources serve or served their purpose for some time and then are replaced, sometimes archived, but often deleted and destroyed. But how could we reuse or repurpose huge piles of old data?

Today, it does not take a genius like Kepler to connect the dots and uncover the data's interdependencies and trends and draw meaningful conclusions from them. We just need to be smart enough to pull the relevant data together and then apply the right tools to connect, analyze, and prepare them for data modeling; ultimately, discovering and revealing the secrets hidden within.

Multiple data models are often built from the same set of data, and the outputs from each model are compared to see whose logic worked best, producing the outputs that most closely match the anticipated reality. Data models often need some fine-tuning to produce optimal

results, and from time to time, the models have to be re-trained with a refreshed set of data to learn about new trends.

After completing data modeling and machine learning, the optimal data model is ready for its real-life application in predicting outcomes, risk modeling, improving productivity through data automation, and many other uses. DCSA is operationalizing multiple practical applications of data science today in partnership with multiple entities.

One such partnership is with the Army Analytics Group (AAG), one of the leading information technology (IT) solutions and research agencies across DOD, to commission the development of tools to prioritize resources and expedite vetting processes. AAG provides problem solving capabilities that involve massive enterprise data integration and analysis, coupled with the most advanced IT solutions.

One critical tool AAG provides is their Person-Event Data Environment (PDE), which removes personally identifiable information (PII) and protected classes from data sets, while linking multiple data sets using new PDE keys. PDE is one way DCSA reduces the risk of their algorithms being biased.

Artificial intelligence (AI) assurance programing is another way DCSA's partnership with AAG ensured the agency's invested tools adopted DOD's five principles of ethical AI — responsible, equitable, traceable, reliable, and governable.

Other projects developed from DCSA's partnership with AAG use various forms of analytics, with prototype capabilities for users and leadership feedback. These prototype capabilities include risk assessments, consistency detection, and key terms.

Risk assessments are products of supervised machine learning algorithms determining how likely an individual is to have their clearance revoked or denied. To ensure the accuracy of these assessments DCSA has invested in multiple machine learning models that sift through large amounts of data looking for patterns of facts that resulted in the decisions made by humans. Risk assessments assist with prioritizing human resources, focusing valuable government assets on the populations that need them most, and can inform future background investigation scopes or thresholds.

Consistency detection models expand on the risk assessment model to assist in determining the accuracy of the model's decision making, as compared to human decision makers. This capability can target cases that vary from the norm, or from what the machine would have recommended identifying areas of variation among the decision-making population. The model will also identify trends across a series of cases, providing insight into applying policies and guidance, or a gap in training. Applying this model to operations provides an additional layer of quality assurance, allowing leaders to identify and address specific training needs for their organization.

DCSA's Research and Innovation team worked with the data science teams to develop a possible solution to expedite the review of cases during the adjudication process. The team found that adjudicators spent a lot of their time scrolling and clicking through documents while scanning for pertinent information. The proposed solution was to develop a tool that can highlight the key terms and create a page of excerpted information for adjudicator review.

Big data provides massive amounts of diverse detailed information. When combined with advanced analytics, natural language processing, data mining, and predictive analytics, they create the most exciting and inspiring discipline in business intelligence.

DCSA stays committed to DOD's principles of artificial intelligence ethics, with the ultimate goal of building credible resources for expanding business process automation, gaining actionable insights into areas of strategic importance, and tools for real-time, fact-based, and informed decisions.


# DCSA'S ROLE IN SECURING DOD SENSITIVE AA&E FACILITIES

**By Jeffrey Cavano and Brian Murphy**
Critical Technology Protection

For over 40 years, DCSA industrial security representatives (ISRs) have contributed to the Department of Defense's Arms, Ammunitions and Explosives (AA&E) program by conducting pre-award security surveys (PASS) and recurring physical security inspections of U.S. contractor-owned, contractor-operated (COCO) facilities that manufacture, test, store, and transport DOD's sensitive conventional AA&E. Although the DOD procuring commands are responsible for overseeing and implementing AA&E requirements, DCSA conducts PASS and inspections to assess contractor compliance with regulatory requirements and contract provisions, when requested.

The security of sensitive conventional AA&E is of the highest importance to DOD. DCSA's evaluation of contractor's security before and after contract lowers the risks of DOD's sensitive AA&E being compromised, sabotaged, stolen, misused, or subject to an act of terrorism or subversion. Sensitive conventional AA&E are designated as Security Risk Category (SRC) I, II, III, or IV. The highest sensitivity level, SRC I, reflects the greatest potential risks to unauthorized use due to its higher casualty and damage effect, utility, attractiveness, and availability to criminal elements. Each SRC is assigned corresponding physical security safeguards to ensure the AA&E items are adequately accounted for and protected.

Just as COVID-19 has affected the rest of the Critical Technology Protection mission through travel restrictions and limited on-site activities, interagency and industry partners can expect changes to DCSA's execution of the AA&E mission at COCO facilities as well. PASS actions for facilities currently in the DCSA AA&E program will be accomplished virtually in collaboration with the contractor's security point of contact to validate applicable physical security safeguards.

At the request of procuring commands, PASS requests for facilities not currently in the DCSA AA&E program will be evaluated for on-site visits. Typically, an on-site request will require the procuring command to provide DCSA with a mission criticality determination, which will require the regional director's approval to support a mission essential activity.

Currently, less than 30 DCSA ISRs serve in the AA&E cadre, providing security oversight for over 165 facilities spread throughout the United States. Each region establishes criteria for selecting and training its AA&E cadre. On October 1, 2020, as part of its reorganization, DCSA consolidated overall AA&E program management at DCSA headquarters under the International-Special Programs (ISP) division. ISP works with the Defense Contract Management Agency (DCMA) pre-award survey managers and regional AA&E coordinators (RACs) to coordinate the management and assignment of AA&E facility inspections with field office chiefs. ISP also coordinates and liaises with the DCMA safety team, DOD procuring commands, and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) to address any unusual situations and compelling needs.

In the near term, ISP will be working with the RACs and the Center for Development of Security Excellence (CDSE) to standardize selection criteria, prerequisites, and standards for AA&E cadre training and qualification. In the future, ISP intends to engage interagency counterparts to standardize and streamline processes and procedures, reach a common understanding of roles and responsibilities through execution of memorandums of understandings (MOU), and interact with industry partners, when requested by the field.


# SPēD CERTIFICATION PROGRAM WINS 2020 BRANDON HALL GROUP EXCELLENCE IN TECHNOLOGY AWARD

**By Kevin Thompson**
**Center for Development of Security Excellence (CDSE)**

In December, the CDSE Security Professional Education Development (SPēD) Certification Program Management Office (PMO) won a 2020 Brandon Hall Group Excellence in Technology Bronze Award in the "Best Advance in Rewards and Recognition Technology" category. The award distinguishes their success with a year-long initiative to transition from manually distributing SPēD certificates of conferral to a completely automated process known as digital badging.

Digital badges are electronic representations of the SPēD certifications and credentials. Using Credly's Acclaim platform — an end-to-end solution for creating, issuing, and managing digital credentials — candidates can manage their SPēD Certification badge(s) digitally, rather than receiving a hard copy certificate.

In June 2020, the SPēD Certification PMO completed migration of the Security Training, Education, and Professionalization Portal (STEPP) learning management system (LMS) to the Pearson Credential Manager, a certification life cycle management tool that manages programs from training through testing and credentialing. The goals were to create a system that would be easy to use for both administrators and end-users, minimize data errors, decrease cost, and accelerate the certification conferral process.

Before the transition, the legacy certification and badging system caused many administrative and user issues. Certification records were stored on two systems (the LMS and a separate certification lifecycle management tool) that required daily data transfers. This resulted in several data transfer errors, which, in turn, caused errors in the certification reporting system. It also prevented the PMO from capturing in-depth candidate information, such as DOD identification numbers, government status identifiers, job series, and job titles.

In addition, the previous conferral process was a labor-intensive 25-step, 90-day manual process that included various administrative activities. Since the migration and new automation, the conferral process has been reduced to a four-step, 48-hour process, issuing more than 8,900 digital badges to SPēD Certification holders through Credly's Acclaim platform since June 2020.

"With the ability to increase the speed of the candidate conferral process, CDSE is more equipped to strengthen the security workforce throughout DOD," said Jason Taylor, chief of the SPēD Certification PMO. "Candidates are now able to pursue additional certifications at a much faster pace. This new expedited process promotes interoperability, which enhances the development of all defense certified security professionals."

Along with being more functional, the migration resulted in a $1.8 million cost avoidance by eliminating the previous STEPP LMS and customizing the "My SPēD Certification" account to manage certification records and deliver digital credentials. The transition will also avoid $87,000 in annual DOD expenses by automating the certificate development and by eliminating the administrative processing, packaging, and mailing burdens.

# CAREER COUNTERINTELLIGENCE EMPLOYEE EARNS SECOND HIGHEST DOD AWARD

Former Secretary of Defense Mark Esper awarded Thomas J. Montero, director for Counterintelligence (CI) in the Western Region, with the Meritorious Civilian Service Award. It is the second highest civilian career award presented by the Department of Defense.

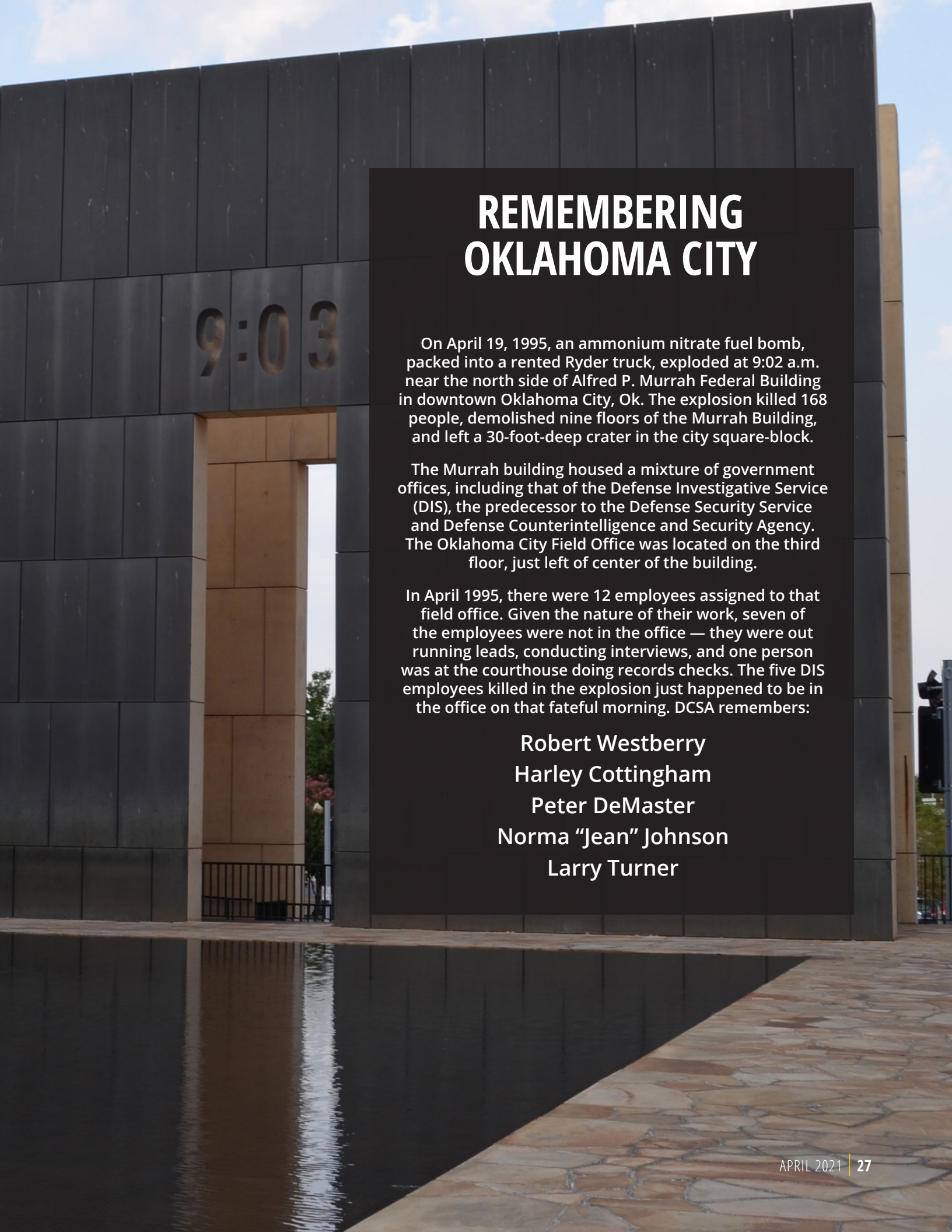
Montero, who has been with DCSA for 19 years, played a major role in developing the Western Region's CI program. Through his threat-driven, intelligence-based, results-oriented approach, the Western Region team garnered nearly 100,000 suspicious contact and insider threat reports originating from cleared industry. His team analyzed and referred reports to partner federal agencies for action that resulted in nearly 2,000 counterintelligence or criminal investigations and operations, indictment of nearly 50 individuals, more than 200 foreign or criminal activity disruptions, and ultimately, the neutralization of numerous human and cyber threats. Further, their collective actions significantly mitigated the loss of proprietary information by an excess of $100 million, according to the cleared companies involved.

Montero is a retired Marine Corps officer with 39 years of combined military and civilian service. His team's ability to describe threat information to cleared industry and emphasize partner engagement has led to many national-level successes with wide-ranging impact. For example, his team identified an export-controlled software being sold overseas by a third party and subsequently enabled retrieval of the software before completion of the sale. Additionally, the team spurred a national-level investigation against a foreign front company that attempted to obtain export-controlled aviation-related data. The team provided intelligence to the FBI, leading to the arrest of the chief executive officer, who had been attempting to illicitly acquire products. They also uncovered three individuals on the national terrorist watch list who had visited a cleared facility, prompting international cooperation leading to the arrest of one individual.

Montero developed a unique Western Region program to complement DCSA's Partnership with Cleared Industry program, which facilitates engagement with senior CI managers across cleared industry. He also engaged directly with senior U.S. government leaders to solidify interagency cooperation, resulting in more DCSA CI agents acting as key liaisons with interagency partners.

Finally, Montero volunteers as the coordinator and chief architect of the Western Region's Operation Warfighter program, which gives wounded warriors an opportunity to gain critical occupational skills through internships with federal agencies during their rehabilitation and transition to civilian life. These internships have enabled many to obtain follow-on employment within the CI or security fields.

***Congratulations, Mr. Montero!***




# REMEMBERING OKLAHOMA CITY

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

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

In April 1995, there were 12 employees assigned to that field office. Given the nature of their work, seven of the employees were not in the office — they were out running leads, conducting interviews, and one person was at the courthouse doing records checks. The five DIS employees killed in the explosion just happened to be in the office on that fateful morning. DCSA remembers:

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

# Defense Counterintelligence and Security Agency

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil

571-305-6562

www.DCSA.mil