DCSA ACCESS

Official Magazine of the Defense Counterintelligence and Security Agency

DCSA RESPONDS TO COVID-19

IN THIS ISSUE

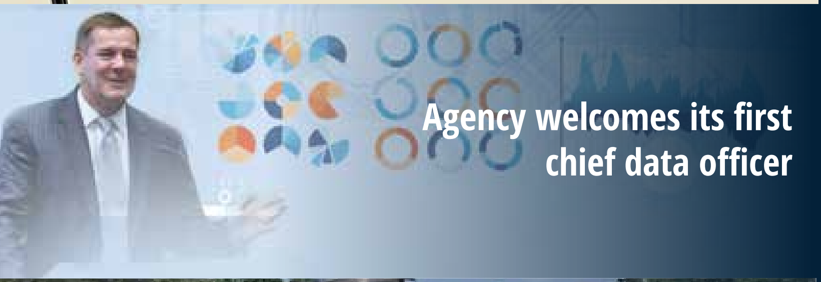
ASK THE LEADERSHIP
Q&A WITH WILLIAM K. LIETZAU

DCSA welcomes new director in a virtual ceremony

DCSA responds to COVID-19

Companies recognized for effective CI programs, enhancing national security

Industrial Security Directorate brings together legacy offices under one umbrella



Agency welcomes its first chief data officer

Engaging cleared academia with risk-based security

VOL 9 | ISSUE 3

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

DCSA LEADERSHIP

William K. Lietzau
Director

Troy Littles
Chief Operating Officer

Jon Eskelsen
Chief, OCCA

Cindy McGovern
Managing Editor

Elizabeth Alber
Editor

Christopher P. Gillis
Staff Writer

Ryan King
Cady Susswein
Andrea Ploch

BARBARICUM
Layout, Editing, and Design

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

All pictures are DoD photos, unless otherwise identified.

FROM THE DIRECTOR

This issue of ACCESS is my first as the director of DCSA. Having now seen up close the great work of this agency, I am grateful to have this forum to share our story. You can learn more about me in a separate article, but I want all our readers to know up front that I could not be more motivated regarding the opportunity to lead this organization. There is no job I would rather have.

DCSA's mission is real: We truly are America's gatekeeper. Unfortunately, our adversaries are real too. And they are getting smarter and more capable by the day. This agency is fighting in a conflict that is taking place here and now — not on some future battlefield. Protecting the trustworthiness of our workforce, facilities, and supply chain is increasingly harder and more complex. And so is the importance of DCSA to our nation's security.

Much of this issue focuses on DCSA's response to COVID-19, as it should. The pandemic has had a profound impact on the nation and how we conduct our daily activities. DCSA is no exception. But it has given us no relief from our mission, and my greatest pride regarding the work of this agency is the fact that we have continued to perform our mission throughout the pandemic — and with greater alacrity and acumen than before the crisis. Perhaps as a consequence of the significant changes the agency has had to deal with in the past two years, our workforce proved itself to be incredibly adaptable. We embraced new ways of accomplishing the mission — whether it was conducting subject interviews, continuous monitoring of cleared facilities, or cyber reporting and analysis. And we succeeded in those adaptations beyond imagination.

Someone recently asked me what I thought the "new normal" would be at DCSA as a result of COVID-19. I hesitate to predict the future, but I have no doubt DCSA will be more effective as we continue to leverage technology and embrace the creativity that brought us to where we are today. We have learned much during this experience, and we are stronger and better for it. And as a result, America is more secure. The same can be true regarding the tumultuous exchanges and protests that currently punctuate our political discourse. Remember that our perspective is a function of our vantage point. Listen to other viewpoints and respect those who have them. We will all be better for having done so.

I look forward to being able to travel again and meet more of the DCSA workforce as well as our government and industry partners. Until then, thank you for your hard work and your continued support of DCSA.

William K Lietzau

William K. Lietzau

Director,
Defense Counterintelligence
and Security Agency

A QUESTION AND ANSWER SESSION WITH THE NEW DCSA DIRECTOR

DCSA Director Bill Lietzau

Editor's Note: The following is the latest installment in a series of features on the DCSA senior leadership team.

The Department of Defense (DoD) named William "Bill" Lietzau the director of the Defense Counterintelligence and Security Agency (DCSA), effective March 30, 2020.

Before coming to DCSA, Mr. Lietzau served as the director of the Personnel Vetting Transformation Office (PVTO), where he managed the transfer of the National Background Investigations Bureau (NBIB) to the nascent DCSA and initiated and led associated transformational efforts.

Before returning to government, Mr. Lietzau was the vice president of a large government services contractor, where he initially served as deputy general counsel, overseeing security, contracting, international trade, and compliance. He later became general manager of an international business unit, providing counterterrorism and law enforcement training and mentorship in over 35 countries, as well as related operations and maintenance, minor construction, and security services.

Mr. Lietzau served over three years as deputy assistant secretary of defense for rule of law and detainee policy and on several U.S. delegations negotiating multilateral treaties. A retired Marine Corps colonel, he served 27 years as an infantry officer and then as a judge advocate, commanding at the company, battalion, and installation levels. An expert in international law, he also served as a prosecutor, defense counsel, and judge, providing legal advice at a combatant command, the Joint Chiefs of Staff, the Office of the Secretary of Defense (OSD), and the National Security Council (NSC).

He earned his Bachelor of Science from the United States Naval Academy and his Juris Doctorate from Yale Law School. He also holds a Master of Laws (LLM) from the U.S. Army Judge Advocate General's School, and a Master of Science in national security studies from the National War College.

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

A: I think what I would stress is — and I have shared this with the workforce — I don't come from any of the legacy organizations that comprise DCSA. Anytime various organizations merge, there is a period of time when members of the antecedent teams may view themselves as competitors with the other constituent organizations, sometimes in healthy competition, but often not. I come from no faction — DCSA is the agency that I am part of, and my loyalty is to every member of the single DCSA team.

Admittedly, maintaining neutrality is probably a bit easier for me than for others. Although I was a facility security officer (FSO) in the distant past and the head of security for a fairly large corporation in more recent years, I've been a citizen dedicated to our nation's security posture for decades. But I do not come from a traditional security background, so I have no preconceived notions regarding competing methodologies. What I do have is experience in organizational leadership and change management — both in government and business. I believe all the skills I've honed in various roles over the years will be useful at DCSA.

As you know, DCSA was only recently established with a major mission transfer in October 2019, involving more than 3,000 government employees, thousands of contractor employees, creation of about 8,600 badges and credentials, and the transfer of more than 100 facilities, 2,000 vehicles, and over a billion dollars to establish a working capital fund. We expect to adopt more personnel, assets, and responsibilities this coming October, so having some experience balancing books is a plus.

Most importantly, however, I want people to understand that I came back to government for one reason: love of the mission. I love this country, and I love working alongside those who share a passion for our national security. As director of the PVTO, I had an opportunity to get out to the field and meet the DCSA staff. In every instance, the passion and dedication of the people performing those functions was evident. I heard the frustration of understaffed and overworked offices, but I never once heard a complaint about the importance or the relevance of the mission. That's not true in every field of endeavor. So, I count myself fortunate to be in such a job.

Q: What are your priorities for DCSA?

A: My number one priority has been and will remain the health and safety of the DCSA workforce. Of course, this only makes sense within the context of performing our mission. And that is what I am most proud of in these first few months as director. Not only has DCSA weathered the COVID-19 crisis, but we have done so while continuing to perform across all of our mission areas. Despite the challenges throughout this period, we continue to work with cleared industry on assessments and accreditations, conduct and adjudicate background investigations at an unprecedented rate, create and distribute counterintelligence products to industry and government partners, and are substantially expanding our online training offerings. We also created an entirely new Continuous Vetting (CV) service offering for the U.S. government.

The bottom line is that we will continue to perform our mission more efficiently and more effectively as we move toward a new normal. I hesitate to use the term "reconstitution" because I don't think we will return to how we did our missions before COVID-19. I have talked with DCSA employees who recovered from having COVID and a conversation with one background investigator has stayed with me. She talked about how well telephone interviews were working and how the savings in travel time was increasing her productivity. Clearly, most of our work is not performed better by phone, but leveraging efficiencies and keeping our mission focus while maintain the health and safety of our workforce is well within our grasp.

My second priority is the full integration of mission and functional components across DCSA. Our nation already merged the DoD Consolidated Adjudications Facility (CAF), NBIB, and Defense Security Service (DSS), and more components are coming under our umbrella in the future. We were brought together for a reason, and we want to take full advantage of the synergies that prompted our union. Transformations as substantial as these almost always involve phases, and this one is no different. We are already looking at potential new operating models, and we will probably need to undergo one or more reorganizations before reaching our goal. It will be difficult, but it is what need to realize our full potential as the preeminent security agency, securing 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.

Finally, DCSA needs to leverage 21st century information technology (IT) architectures to successfully match our adversaries and accomplish our mission. Step one has been to reset the goals and schedule of our nascent National Background Investigation Services (NBIS). The massive undertaking has been frustrated by frequently changing requirements, which are sometimes inadequately resourced. We need to change that and ensure we deliver capabilities consistent with the promises we make. But that is only the beginning. During the next few years, we will be improving and deploying a number of IT capabilities — from Defense Information Security System (DISS) to a new and improved DITMAC System of Systems (DSOS) — that should posture us for optimal mission performance.

Q: Can you talk more about those next transfers? What are they and what can we expect to see?

A: First will be the Program Executive Office (PEO) for NBIS, which I just mentioned. In 2016, the Defense Information Systems Agency (DISA) was tasked to design, develop, test, field, operate, maintain, and secure an IT system, or suite, to conduct background investigations for civilian employees, military service members, and government contractors. In June 2019, the secretary of defense directed the DISA component building NBIS move to DCSA along with DISA's NBIS PEO. The Defense Manpower Data Center (DMDC) will be transferring to DCSA a number of other IT capabilities that support the department's vetting mission and can be folded into the NBIS capability.

Additionally, this year, the deputy secretary directed the transfer of the National Center for Credibility Assessment (NCCA) from the Defense Intelligence Agency (DIA) to DCSA. NCCA is the government's premier educational center for polygraph and other credibility assessments technologies and techniques. Combining it with the National Training Center (NTC) for background investigators and the Center for Development of Security Excellence (CDSE), the new educational arm will help establish DCSA's new National Security Learning Center.

And finally, DCSA had been "buying back" some legacy IT support services and some financial management services from the Office of Personnel Management (OPM). We have collectively agreed that the current buy back arrangements are not sustainable, so we plan to transfer the personnel, resources, and responsibilities to DCSA as soon as practicable. There are a few other potential missions in the mix, but any way we look at it, our next year will be busy.

Last year's transfer of NBIB and DoD CAF was a huge success, and it rightfully received a lot of positive attention. I am incredibly proud of what was accomplished with no disruption to mission and no added cost to the taxpayer. This set of transfers will likely not receive the same visibility outside our community, but they may be even more complex. My goal is to be as open and transparent in these transfer activities as we can. We are working from detailed schedules and with carefully identified milestones. I am confident that we will be successful.

Q: Are you looking at organizational changes at DCSA to support these new missions?

A: Yes. As mentioned earlier, a transformation of this magnitude almost always involves phases and one or more reorganizations. We are America's gatekeeper — but the complexity of that mission is not what it once was. And we cannot successfully accomplish our increasingly complex mission without adjusting. We have to work differently to gain efficiencies and synergies needed to meet the threat. The world is changing, and we have to change faster.

All that said, the change will be deliberate and methodical. Mission always comes first. I know there is concern about the field and regional structures. At present, the background investigation and the technology protection components are doing business in different ways. Simply shoving them into adjacent offices is not likely to yield the efficiencies we need. I cannot risk any degradation to the mission in the field while we adjust, so we will ensure that any new operating methodologies are carefully tested, and field mergers are thoughtfully planned.

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

A: I'd like to repeat a reflection I shared the day I took over as director. Reflecting on a career-oriented board game I played as a child, I recalled that the game required choices regarding levels of power, money, and fame (players had to choose among them). Unlike in the game, it seems like DCSA does not really offer an excessive amount of any of these three potential motivators. But we all enjoy an honorable vocation. We don't do what we do because being a gatekeeper is glamorous. But everything we do is directly relevant to the national security of this great nation. That is not something many can say about their jobs. And being able to work alongside others who value it is a blessing. Thank you for it.

DCSA WELCOMES NEW DIRECTOR IN A VIRTUAL CEREMONY

In a virtual ceremony broadcast to the workforce on March 30, William (Bill) Lietzau assumed the position of director of the Defense Counterintelligence and Security Agency (DCSA). Lietzau replaced Acting Director Charlie Phalen who had served in the position since June of 2019. The adaptation to a virtual ceremony was taken in response to the COVID-19 pandemic, which mandated social distancing and had almost the entire agency workforce teleworking. The events still reflected, however, the trappings of a typical change of command or directorship ceremony with remarks by senior leaders and the passing of the agency's flag or colors.

Under Secretary of Defense for Intelligence & Security (USD(I&S)) Joseph Kernan participated virtually and offered remarks to the workforce. Kernan asked that the workforce not judge the importance of the event by the lack of a physical presence and noted that the workforce is using technology such as video teleconferencing (VTC) to conduct its investigative mission.

He then thanked Phalen for his dedication and commitment leading the transfer of the investigation mission to the Department of Defense (DoD). Kernan commended Phalen for transforming DCSA into the expansive organization it is today. "DCSA has a no-fail mission and you have set it up for success," Kernan said.

In closing, Kernan said to Lietzau, "Remain vigilant in protecting the health of the workforce. Know that the department will continue to support you and have confidence in your leadership."

Following his remarks, the certificate of appointment was read and Elizabeth Hoag, director of the Human Capital Management Office (HCMO), administered the oath of office to Lietzau, signifying his appointment as the director. Once the agency flag was passed, Phalen bid farewell to the workforce.

DCSA Director Bill Lietzau recites the oath as part of the oath of office ceremony.
(Photos by Christopher P. Gillis, OCCA)

Phalen remarked, "I have been honored over the last three and a half years to be part of, first, the National Background Investigative Bureau (NBIB) team as we focused on some significant challenges. Then, for the past nine months, with the whole DCSA team as we worked on combining all the pieces into one very large enterprise."

"I am proud to say in both instances, borrowing from the Elle Woods movie character: we did it!" he said. Phalen said there were still "potholes in the road" but the fact that the agency has come so far is a great testimony to what the workforce has accomplished.

In closing, Phalen said, "Thank you for your confidence and support, thank you for getting us to where we are

Assembled for the change of directorship ceremony are (from left to right):
former DCSA Acting Director Charlie Phalen, Chief Operating Officer Troy Littles, Director Bill Lietzau, and Chief of Staff Ellen Ardrey.

today, and thank you for what you do every day to make this country more secure. I truly look forward to reading more about your continued exploits and progress in the future."

In his first remarks, Lietzau noted the new operating normal as well. "I have been to many changes of command and normally the new guy doesn't say much because he doesn't know much. But this is not normal," he said.

"First, I am truly honored and grateful to be here," said Lietzau. He added that upon coming back to DoD less than a year ago, he no idea that he would end up here today. "Although I was not seeking it, there is no job I would rather have. Secretary Kernan, thank you for your trust. Thank you for being part of this ceremony," he continued. "Mr. Reid, thank you for hiring me in the first place."

Lietzau thanked Phalen for this leadership during a complex and difficult transfer. "No single factor was more responsible for the success of the Defense Security Service (DSS), DoD Consolidated Adjudications Facility (CAF), and NBIB transition into DCSA than Admiral Kernan's choice of Charlie Phalen as its acting director through the transfer," Lietzau said. "Charlie has been the steady hand and thoughtful leader our nation needed through what has been one of the most significant organizational mergers our government has seen in the past decade. Thrice retired now, this country owes him a great debt of gratitude."

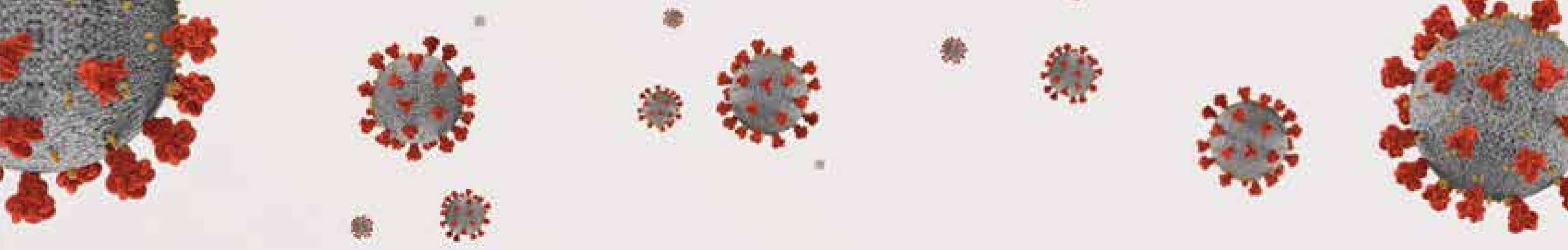
Lietzau remarked that he would prefer to meet the workforce in person, but it was unclear when that would be feasible. So, instead, he used this opportunity to explain why he was excited to be at DCSA. "After over 30 years in government, and half a decade running a business, I came back to the government for one reason: love of the mission. I love this country, and I love working alongside those who share a passion for our national security," he said. "As director of the Personnel Vetting Transformation Office (PVTO), I had an opportunity to get out to the field and meet a few of you — in every instance, the passion and dedication of the people performing those functions were evident. I heard the frustration of understaffed and overworked offices, but I never once heard a complaint about the importance or the relevance of the mission. That's not true in every field of endeavor."

Lietzau said his biography doesn't list working at NBIB nor at DSS. "I am an outsider to both — from neither. I am joining DCSA, the agency you are part of," he said. "It is a transforming agency that must be better integrated. And yes, my role will be to bring about change. We will be changing." Lietzau added that moving forward, circumstances may cause us to function differently, and we will want to operate differently.

"We need to look to the new normal," he said. "Not only a post-COVID normal but a more efficient and effective normal that reflects the synergies for which we were brought together. Through all of it, our essential mission as America's gatekeeper will not change."

"This mission is real," added Lietzau. "Our adversaries are real, and they are getting smarter. Protecting the trustworthiness of our workforce, facilities, and supply chain are getting harder and more complex. And DCSA is becoming more important by the day. If you want a role that is significant, that doesn't just claim to protect — but actually does protect — our national security every day, you can find no better organization in which to work than DCSA. That is why I love this job."

In closing and reflecting on a quote from Alexander Pope's "Essays of Man" on whether one's birth or position — peasant or prince — made them more or less honorable, Lietzau said the work that DCSA does could not be more honorable. "And I am proud to have joined your team," he said. "I will endeavor to 'act well my part' for this agency and for you. Our country needs you. Stay healthy. God bless you, your families, and our great nation during this difficult time."



DCSA RESPONDS TO COVID-19

In late February, the new coronavirus, COVID-19, became a daily news event and DCSA began a multi-pronged approach to monitor and assess the quickly developing situation. In mid-March, as schools and businesses began to close, DCSA followed suit, and employees scrambled to take home laptops and other IT equipment to prepare for maximum telework. For many employees, Friday, March 20, was the last time they saw their co-workers, reporting to their home offices the following Monday to develop a new operating model for themselves, their teams, and the agency.

While any major event offers challenges, it also offers opportunities. Director William Lietzau, who assumed DCSA command during a virtual ceremony, said the agency's workforce has not only met these challenges head-on but has far exceeded expectations. "I think this organization has been primed for change for a while," he said. "That mindset has helped us during the COVID-19 response." Lietzau added that every mission area has continued to work, and in some cases, develop efficiencies that can be adopted into the future.

The following pages capture some of those efficiencies as well as the professional and personal changes the DCSA workforce has made to continue to complete the mission and serve their communities.

COVID-19 Working Group

One of the first steps DCSA took in responding to COVID-19 was establishing a dedicated cross-functional working group consisting of representatives from Security, Mission Assurance, Human Capital Management Office (HCMO), Office of the Chief Information Officer (OCIO), Acquisitions, Office of Communications and Congressional Affairs (OCCA), Logistics Management Division (LMD), Safety and Occupational Health, and various other offices.

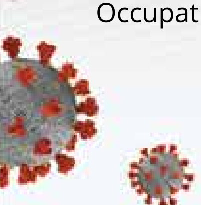
The working group, led by Delice Bernhard, director for Security, Insider Threat, and Mission Assurance, met daily to discuss the latest developments and review and interpret the various Health Protection Condition (HPCON) measures, COVID-19 related policy, and guidance from the White House, the Secretary of Defense (SECDEF), the Under Secretary of Defense for Intelligence and Security (USD(I&S)), and the Centers for Disease Control and Prevention (CDC).

The team also collaborated on a daily workforce message, including everything from operational updates and guidance, telework tips, frequently asked questions, and a guide on how to make face masks. The communications team established dedicated COVID-19 pages on the internal employee websites that included the workforce message, as well as graphics and tools to understand the HPCON conditions and COVID-19 terminology.

HCMO delved into the complexities of weather and safety leave to ensure employees understood the program, shared tips on effectively working remotely, and highlighted Employee Assistance Program (EAP) resources to promote mental wellness. Meanwhile, LMD ensured more than 100 facilities were closed following caretaker status policies and shared guidance on expiring vehicle license plates.

With teleworking as the new norm, employees had to learn to conduct business using new methods and tools. To that end, OCIO started pursuing various collaborative IT tools that allow employees to continue to do their jobs, providing "how-to" guides on accessing voicemail remotely, mapping a network drive, and approved web camera use. Acquisition personnel applied the guidance to the federal workforce and oversaw the contractor workforce.

The Center for Development of Security Excellence (CDSE) saw a large growth in eLearning course completions during the COVID-19 crisis, increasing from



136,000 in March to 164,000 in April. Total completions were over 740,000 to date, or 100,000 more than the same time last year. Likewise, the number of times students have accessed the CDSE performance support tools, case studies, job aids, webinars, shorts, and toolkits more than doubled from 41,000 in March to 119,000 in April.

Administering COVID-19 tests

Bob Dalton dons his protective gear before administering Coronavirus antibody tests.

In August 2018, Denver Field Office SAC Bob Dalton and his wife Dorie became volunteer firefighters with emergency medical response training at the Genesee Fire Rescue in Golden, Colorado. They did it as a way to serve their community and neighbors. In April of this year, when their county obtained a supply of COVID-19 antibody tests, they needed medically trained volunteers to administer the tests and analyze the results. Naturally, the Daltons stepped up to help the community.

In April, over 1,200 people were tested at their volunteer sites. To protect themselves during this process, the Daltons wore Tyvek suits, N-95 masks, glasses or goggles, face shields, and gloves in addition to testing themselves weekly. The Daltons plan to continue volunteering at the testing center as long as they are needed. "Between volunteering at the testing center and continuing to support our neighbors' emergency fire calls, we're at least able to feel like we're helping in some small measure," said Dalton.

Personnel Vetting adapts

COVID-19 made it somewhat difficult for investigators to satisfy some investigative coverage requirements, including personal interviews, subject interviews, source searches, and reviewing required record information. Many businesses were closed or no longer allowed visitor access. In response, Personnel Vetting (PV) issued operational guidance that allowed for temporary adjustments in background investigation methodologies, such as expanding previously issued guidance on the use of video teleconferencing (VTC) and conducting telephonic interviews.

The pandemic presented another challenge to the Personnel Vetting mission, as many of the fingerprinting sites were closed. The Office of Personnel Management (OPM) issued temporary guidance to address the challenges federal agencies were having collecting fingerprints. For agencies that were able to collect prints, they were encouraged to continue to do so. For agencies experiencing difficulties, temporary measures allowed submission of investigation requests without the required fingerprints until fingerprint processing was feasible — no later than the date of termination of the temporary guidance from OPM.

On April 3, USD(I&S) issued guidance stating that Department of Defense (DoD) components would continue, to the maximum extent possible, collect and process fingerprints, follow established guidelines for vetting new hires, and determine eligibility for issuance of personal identity verification (PIV) credentials.

DCSA implemented procedural changes to allow processing of investigation requests from non-DoD agencies without fingerprints. Additionally, the Federal Investigative Records Enterprise (FIRE) created National Student Clearinghouse (NSC) accounts for PV personnel to conduct education verifications and a new workload tool that allowed offices to manage the searches they conduct. This eliminated the need to physically mail out over 2,000 vouchers. With more work being done telephonically, the importance of the call centers became paramount.

Employee recognized by White House

Security Assistant Stacy Babcock from the Boyers Security Office was recognized for her "prompt and efficient service, professionalism, and congeniality" in response to an investigator verification inquiry from a senior advisor to the national security advisor in the Office of the Vice President (OVP).

A standard duty for the Boyers Security Office is to answer inquiries received through the investigator verification line, a service that accepts calls and emails from the public to verify the identity and confirm the credentials of any background investigator. Since the COVID-19 restrictions were put in place, more investigation activities have happened virtually, and there has been a significant increase in the number of inquiries the team is receiving. The inquiries went from 823 in February to 1,488 in March and then climbed to 2,869 in the first three weeks of April. A sudden surge like this could easily overwhelm an office and result in failure. A team of four individuals met this challenge with gusto and continued to complete their other duties as well. The OVP security advisor noted that his call was returned "within a few minutes" and that Stacy is "a sterling representative" of DCSA.

Applicant Knowledge Center handles e-QIP inquiries

Customer & Stakeholder Engagements (CSE) within Personnel Vetting began working on a concept for an Applicant Knowledge Center (AKC) in Boyers, Pennsylvania, to receive and resolve all issues for applicants using the National Background Investigation Services (NBIS). In anticipation, DCSA hired 10 personnel who began work in February and were trained on the Electronic Questionnaires for Investigations Processing (e-QIP) to gain experience assisting agency users.

The Vetting Risk Operations Center (VROC) operates a call center to assist DoD customers, but the VROC's call center was not capable of receiving calls while in a telework status. CSE and VROC immediately began collaborating on a resolution in March to shift calls from VROC to AKC and the newly hired staff. While there was an initial surge of calls that had the AKC operating at near 100% capacity, the call volume has since subsided to a more manageable state. The response has been positive with callers expressing gratitude for having live support to walk them through their unique situations.

Efficient processing of cases

Most of the Personnel Vetting directorate's workforce has been accustomed to using telework as a standard part of their schedules before the COVID-19 crisis. However, that didn't mean that the expanded telework orders didn't have an impact on operations, especially when coupled with the social distancing recommendations.

The Personnel Vetting Quality Oversight team collect cases using a drive-through system at Fort Meade, Md.

Teams across PV had to devise plans to keep their operations going while also keeping employees safe and adhering to social distancing. The restrictions provided an opportunity for the PV components to share and leverage each other's ideas and best practices to quickly implement safe and practical workarounds.

One example was the efforts of the PV Quality Oversight team, which needed a plan to minimize the amount of personnel in the office while also ensuring that all reviewers and adjudicators had the materials they needed to continue working. As plans were developed and communicated, they were also shared among other DCSA teams for leaders to adapt and implement as needed.

The Quality Oversight team developed a process for their investigative case analysts and security assistants at Fort Meade and Boyers to pick-up and drop-off their cases with minimal to no contact. At the Personnel Investigations Center (PIC) in Fort Meade, they were even able to institute a drive-through system, in which team members did not need to get out of their cars.

Facility Assessments Continue

The Industrial Security workforce also maximized telework. Instead of the normal Enhanced Security Vulnerability Assessments (ESVAs) or other on-site engagements, it implemented a Continuous Monitoring (CM) strategy to identify which cleared facilities were continuing operations, offer guidance and assistance, and assess the current security situation using solely virtual communication. This approach allowed industrial security representatives (ISR) to use alternative methods to relay security requirements to industry and to proactively identify areas that need an on-site visit when circumstances allow. As the field workforce returns, they will prioritize visits to companies with potentially serious industrial security deficiencies or those that need immediate support.

Stitching face coverings for family and friends

Stacy Elliott (left) stands with her father and husband in masks that she created.

When CDC and DoD issued a directive to use some form of facial covering, Stacy Elliott, spouse of Irving Field Office CISA Jeff Elliott, began making masks to assist those in need. Mrs. Elliott, who owns a sewing company, saw the need and responded by using quilting materials and her sewing skills to make much-needed personal facial masks. She has received requests from family, friends, and friends of friends. With a daily production output of 20-25 personally designed masks, so far, Mrs. Elliott has created over 125 masks, with requests for over 120 more. Her masks have reached people in New York, Georgia, North Carolina, Ohio, West Virginia, Pennsylvania, Florida, Texas, and beyond.

Southern Atlantic quick response

When COVID-19 stay-at-home restrictions were implemented, Special Agent-in-Charge (SAC) Joseph Kroto Jr., in the Columbia, South Carolina Field Office, and several of his agents jumped into action to ensure they could continue to conduct investigations. Special Agents Despina Washington and David Hamrick, also from the Columbia Field Office, coordinated with the U.S. Army Basic Training Brigade at Fort Jackson. Meanwhile, Special Agent Scott Gardner coordinated with Marine Corps Basic Training at Marine Corps Recruit Depot in Parris Island.

Interviewing recruits during basic training saves the military time and money, while simultaneously ensuring that an individual is a trusted insider before they have access to national security information or begin working in a critical position. When recruits leave, follow-on training often requires a security clearance. Without it, the individual is placed on hold, which delays training and affects the military's readiness. Due to the agents' efforts, processes were quickly established to facilitate telephone interviews at optimal times in the basic training cycle, and the Parris Island communication team was able to set up a private phone center for recruits.

Additionally, SAC Sydnee Vinson from the Georgia Field Office coordinated with Case Analyst Jodie Rodgers at the Federal Investigative Processing Center in Boyers to provide Southern Atlantic-area field offices with a roster of recruit training installations in the area after their cases had been scheduled and assigned. As a result, they were able to quickly reschedule those cases.

Conducting CI outreach via Adobe Connect

After the initiation of maximum telework across DCSA, counterintelligence special agents (CISA) in the Western Region implemented Adobe Connect as a solution to provide effective and timely counterintelligence (CI) education and outreach to cleared contractors. The Western region CISAs drafted operating procedures and field user guides to distribute to other DCSA regions. All other regions are now using video teleconferencing for outreach purposes. For example, CISA Mark Zahner, from the Hanover Field Office, conducted a cyber threat webinar using Adobe Connect to educate 40 facility security officers (FSOs). Southern Region CISAs held weekly conference calls to connect with FSOs throughout the region. North Region CI received kudos from a cleared company for a briefing that CISA Abigail Madden gave via Adobe Connect. They were impressed by the content of the briefing and excited to use the option in the future if travel becomes difficult again.

Special Access Program guidance

In response to a government customer's inquiry, the DCSA International and Special Access Program (SAP) office coordinated with the NISP Authorization Office (NAO) to develop and distribute a COVID-19 guidance memo. NAO's memo provided operational guidance for maintaining DCSA-authorized SAP information systems at contractor locations and was distributed to DCSA information systems security professionals and government program security officers.

Curbside service for equipment

The DCSA Asset Manager Centers (AMC) and LMD continued to operate with minimal manning to ensure that all DCSA employees received their equipment requirements. The Fort Meade AMC offered social-distanced curbside service to issue and receive equipment for teleworkers. The AMCs at Quantico, Fort Meade, and Boyers also sent equipment directly to employees' home addresses to alleviate the need for staff to travel to work sites for equipment. Steven Turner at Quantico, Marty Terro at Boyers, and Shane Jolley and Michael Little at Fort Meade, have been stepping up, coming to work masked and ready to provide the best customer service to agency employees.

Fax Brigade

With offices closed and access heavily restricted, agents in the Denver Field Office were left with a very uncommon problem in this day and age. Under normal circumstances, many investigation records (police, court, and employment verification) are obtained in-person. However, due to COVID-19, an increasing number of records were arriving via fax. However, many of these records cannot be sent through Voice over Internet Protocol (VoIP), wireless fax, or email due to personally identifiable information (PII) protections.

Three special agents — Diana Boutwell, Ralph Bammert, and Ed Barthlome — were equipped with landlines and fax machines in their home offices and stepped up to help the team. After confirming that their home offices were in a room that could be locked as an additional layer of protection, they received approval from their area chief, and the field office's 19 agents were divided into three teams working with these new fax contacts, or the "Fax Brigade", as they have come to be called.

In addition to their regular duties as special agents, the Fax Brigade received files to scan and fax as requested. The ability to continue sending and receiving faxes allowed the agents to complete their cases without having to write-off items or place cases on hold due to an inability to access records.

Handmade art for hospital worker relief

Jason Elmore shows off one of the items auctioned to support local emergency room employees.

CISA Jason Elmore, from the Irving Field Office, put his woodworking hobby toward a greater cause. Elmore created a week-long auction for some of his items to donate 100% of the proceeds to a local hospital's emergency room personnel. Elmore was able to auction five items, raising a total of $550. He purchased a Visa gift card for the emergency room staff to be used for coffee, food, or anything else the section needed.

Industry IT systems were secured

Information systems security professionals (ISSPs) also found ways to adapt to a new operating environ-ment. They worked to extend Authorizations to Operate (ATOs) and authorize and audit variances that were due to expire. This allowed DCSA to work with industry to ensure operations to support the warfighter and classified programs were sustained. ISSPs worked with their industry partners to establish standard operating procedures (SOP) to specify how systems should be protected during potential dormant states and how industry would begin immediate patching and update installations upon return to service. DCSA continues to perform assessment and authorization activities while only delaying, deferring, or rescheduling onsite activity.

Supporting hometown and community

Marguerita Ramirez (left) works with an employee of HOPE Charitable Services to make salads to accompany to-go meals for those in need.

When Marguerita Ramirez from the Industrial Security Directorate (ISD) couldn't find hand sanitizer in stores, she decided to make her own. After sharing a photo of the homemade sanitizer with her mother, she found out that the shelves were bare in her hometown of Portsmouth, Virginia. To help prevent the spread of COVID-19, she made 50 bottles of hand sanitizer and gave it to her home church for those in need.

She also assisted her church with feeding the homeless by reaching out to friends and spearheading a small group of people in a cross-agency effort to provide over 100 hot to-go meals. She got help from a team of civilians and military from DCSA, U.S. Marine Corps, U.S. Air Force Office of Special Investigations, Naval Criminal Investigative Service, Department of the Navy, Census Bureau, and U.S. Army to provide a nutritional meal that was balanced, affordable, filling, and relatively easy to cook, serve, and hand out. In late March, the team delivered the food, and the church served hot to-go meals to 126 people.

Supporting essential workers

During the quarantine, North Region CI personnel provided over $500 to source and supply N-95 respirator mask, nitrile surgical gloves, and disinfectant spray to local rehabilitation centers, nursing homes, medical personnel, immunocompromised individuals, and homeless shelters. In one instance, a North Region CI employee reached out to a company that supplies needed chemicals to local medical device manufacturers when they ran out of protective equipment. They were able to find a reliable source of protective equipment for the chemical company, preventing a potential halt in life-saving medical device production.

Full-time area chief, part-time PE teacher

As an area chief for Western Region Field Operations, Bob Dubek is a remote worker who was already acclimated to working from home due to office space limitations. Yet, with the entire family home, the current restrictions provided unexpected challenges with new family support opportunities. His wife began homeschooling their kindergarten grandson, and Bob stepped in to assist as his grandson's physical education teacher. Bob has been scheduling times throughout the day to either walk or bike with his grandson, which extends his workday but eases his stress and minimizes mental overload. "Between March and into April, I've accumulated over one million steps, or 570 miles," said Dubek.

Retirement ceremony via social distancing

SAC Scott Badger from the Fayetteville-Fort Bragg Field Office spent his last day as a federal employee on April 30 at home due to COVID-19 restrictions, but his leadership, team members, and family didn't let the day go by without a show of appreciation for his 33 years of service to the background investigation mission.

The first gesture was a ceremonial farewell conference call with 80 participants from across the country, including field operations senior staff members, agents, and SACs from the four field office teams that Scott supervised over his career. As a bonus, the call coordinators were able to include Scott's family members, including his wife and his two daughters, who live out of state. His daughters prepared a video that featured well wishes from his current staff as well as retired teammates. The video also included a special thank you for Scott's many years of service from one of his favorite former National Football League players: Hall of Fame Defensive End Bruce Smith. To end Scott's last workday, his team members at Fort Bragg coordinated a series of fire trucks to drive down the street with lights and sirens blaring. Twenty or so staff members followed suit in their cars, waving and yelling congratulatory comments as they passed his house.

Building morale through music

Employee morale is always a concern during times of stress and significant change, and the COVID-19 crisis was no exception. Personnel Vetting's Kansas City 2 Field Office used music to ease anxiety and come together as a team. To help keep spirits high, 11 team members collaborated to create and share two playlists amongst their field office. The motivational playlist was built for days when the going gets tough and included songs like "Shoots and Ladders" by the metal band Korn and "I Won't Back Down" from singer-songwriter Tom Petty. The quarantine playlist is filled with songs to remind the team members that they're all in this together, including "Working Night and Day" by pop legend Michael Jackson and "Don't Stand So Close to Me" by the rock band The Police.

Team member and playlist contributor Kerry Anderson shared, "I was introduced to songs and artists from music genres I don't normally listen to. Sometimes, I find myself typing to the rhythm of some of the songs."

Bring your own breakfast – virtually

Under normal circumstances before the pandemic, a few agents from teams within the Orlando Field Office would get together in small groups about once a quarter for breakfast to catch up and talk through any updates or concerns. With COVID-19, there was no opportunity for these gatherings to occur.

A month into the social distancing restrictions, Special Agent Douglas Oyler began to feel the effects of isolation and realized that something was missing — he hadn't seen a single coworker in over a month. With management support, Douglas scheduled an Adobe Connect session and invited his agents from across the Orlando Field Office to join him for a "bring your own breakfast (BYOB)" virtual gathering. Unlike their previous in-person gathering, this virtual session allowed agents who would not normally be able to attend due to location or other restrictions to share their thoughts and ideas. The gathering lasted for about an hour and had nearly 20 participants. No major issues were solved, but that wasn't the focus of the gathering. The agents were able to connect over their common bond and just share a moment of normalcy and understanding.

Supporting neighbors with food, books

St. Louis Field Office Special Agent Jeff Lapp and his wife Tiffany have always valued community involvement and considered it a priority to find ways to give back. Their community set up several micro-pantries to help those in need with food, cleaning supplies, toiletries, paper products, baby items, and books. Jeff and Tiffany contributed an SUV full of items to micro-pantries near their home several times and are committed to continuing these donations until things start to normalize.

The couple has also been closely involved in literacy initiatives through the Northside Children's Community Library since 2017. They gave, collected, and redistributed approximately three boxes of gently used books per week, or more than 150 boxes per year. In recent weeks, the Lapps worked to set up a Little Free Library outside of the high school near their home, where community members can pick up and drop off books. Additionally, they have been working to coordinate a book delivery program where families in their neighborhood can receive books by porch drops.

Left: The Lapp family provides gently used books for all ages.

Right: The micro pantry, set up by the Lapps, contains donations for those in need in the community.

COVID-19 HAS IMPACT ON INTERNATIONAL MISSION

By Terrill Hines
Personnel Vetting International Activity Program Office

In January, the International Activity Program Office coordinated the deployment of 21 special agents to Japan, South Korea, Germany, Italy, and Bahrain. Little did the office at Fort Meade know that the Coronavirus 2019, or COVID-19, would impact the overseas mission just a few short weeks later.

During the early days of COVID-19, International Activity faced a number of uncertainties and questions about the safety and health of the deployed agents. Because COVID-19 was primarily overseas, International Activity gathered warning level information supplied by the Centers for Disease Control and Prevention (CDC), the U.S. Department of State country advisories, and the military base guidance where the agents were stationed. Daily activities included tracking base-level actions and corresponding with the agents overseas. Additionally, reports were provided daily to DCSA senior leadership as well as Security and Mission Assurance on the status of these agents.

After the CDC raised the geographic risk transmission levels for the COVID-19 virus in Italy, South Korea, and Japan, DCSA decided that agents assigned to these areas should return home. Receiving notification from the International Activity Supervisory Agent in Charge Dave Brawley, the agents secured return flights. As the travel health notice warnings increased, so did the immediate risk to agents located in other countries. As a result, the DCSA assistant deputy director — operations issued a directive for the return of all agents from overseas. Upon arriving at their homes, each agent completed 14 days of self-quarantine before returning to a DCSA facility.

“It was a whirlwind. Go from eating German food one day to being in quarantine in the United States the next,” said Special Agent Jacqueline Schwabenbauer, who was stationed at Ramstein Air Base, Germany.

After spending 22 years in the U.S. Army, Special Agent Christopher Real was used to it. “It was fine,” he said on his return from Okinawa, Japan. “Had to hurry, pack up, and leave. Departure went pretty smooth overall when changing flights in the Defense Travel System (DTS).”

With all agents stateside, the International Activity continues its overseas mission using expanded virtual interview platforms. We look forward to returning agents overseas when travel is permitted again.

COVID-19 | BY THE **NUMBERS**

While every office was challenged by COVID-19, the entire agency looked to the Office of the Chief Information Officer (OCIO) to keep the Defense Counterintelligence and Security Agency (DCSA) networks running. Without the ability to connect to a secure internal network, the workforce would have been unable to access email, share files and information, obtain help desk support, and retrieve saved data. In short, they would have been unable to function remotely. Through it all, OCIO rose to the challenge and has the numbers to prove it. The following are some of the statistics tracked by the OCIO team since mid-March.

DEPLOYED OVER

270

TYPES OF PERIPHERALS,

including web cameras, headsets, monitors, keyboards, and mice in support of telework initiatives.

PUBLISHED

"HOW TO" GUIDANCE

and set up and monitored

314 "MEET ME" CONFERENCE LINES

in support of telework initiatives.

PROVISIONED OVER

200 NEW "MEET ME" CONFERENCE BRIDGE LINES

for the agency in support of telework initiatives and **developed a selectable options template** to customize conference line preferences.

PROVISIONED THE

SINGLE LARGEST ONE-TIME "MEET ME" LINE IN AGENCY HISTORY

in support of the director's town hall with

4,072 personnel through AdobeConnect & **1,900+** through the conference line dial-in.

CREATED

30 "HOW TO" SELF-SERVICE KNOWLEDGE ARTICLES ACCESSIBLE VIA REMEDY

— currently viewed over **617** times.

PROVIDED

VIRTUAL PRIVATE NETWORK (VPN) CAPABILITIES TO SUPPORT THE ENTIRE AGENCY WITH ACCESS TO ALL DCSA SERVICES DAILY.

Successfully increased the VPN concurrent capability from **2,000 to 8,000** within 26 hours to provide access to all DCSA services as COVID-19 emergency response.

Enabled remote pre-production VPN network access to developers and testers with an average of **15+ developers and testers** daily.

PROVIDED

VIRTUAL DESKTOP INFRASTRUCTURE

(VDI) access from home, with an average of over 90+ users logins daily.

ENABLED

JABBER VOICE SERVICES

for Service Desk and Knowledge Center staff to provide remote support.

PROVIDED

GLOBAL VIDEO SERVICES

(GVS) capabilities for over 100 users.

PILOTED **ZOOMGOV** and provided support, webcam, headset, and software for over

40 PILOT USERS

for web conferencing and video conferencing services.

PILOTED **DoD COMMERCIAL VIRTUAL REMOTE** (CVR), a central place for unclassified virtual collaboration, for over

1,000

REGISTERED DCSA USERS.

CONTRACTOR RESILIENCY DURING COVID-19

By Garrett L. Speace
Industrial Security Directorate (ISD)

I recently spoke with a contractor to gauge how their business and operations were impacted by COVID-19. I was surprised to hear that there was minimal impact on their ability to support their customers. When asked how they avoided the issues some of my other assigned contractors were running into, they said they brought everyone together to discuss what they needed to do to continue to meet their contractual requirements, support their customers, and protect national security.

Their first conversation was with the customer to determine which items on their task order were mission essential so they could prioritize those items. They then contacted their contracting officer to modify their contract to allow for telework for any work that could be accomplished without being on customer site. Previously, the contract did not allow for telework or remote support. It's one thing to have the technical capability to do these items remotely, and it's another to be contractually allowed so that it doesn't impact the contractor's performance ratings.

The program manager and the facility security officer (FSO) then discussed how they would staff the customer sites while taking into account social distancing, new COVID-19 operational security requirements on the fleet, their readiness, and the new requirement to shelter-in-place for 14 days before deploying or returning from a deployment. All the while, maintaining a cleared workforce that could support the fleet while other employees were in a mandated shelter-in-place.

There's an old saying that "failing to plan is planning to fail." We do not live in a world without challenges and uncertainty. The Department of Defense (DoD) has gone through sequestration, two shutdowns, and now COVID-19, just in the past decade. Contractors that wargame or project possible events find themselves more prepared during these times of change because they have already gone through the practice of adapting to the new environment, changing their operations, and identifying gaps if they were to operate differently.

A smart adversary takes advantage of chaos and confusion. There has been no shortage of news articles about the vulnerabilities to information technology solutions that have become household names since the stay at home orders were issued in most states. The contractors that planned for these types of events already have the solutions that meet their customers' security requirements. This allows them to continue working instead of spending more time and resources trying to get up and operational again. Resiliency is the ability to bend but not break. Some contractors have adequately prepared for these types of events, but there will be many lessons learned as we progress through these unprecedented times.

NSLC
National Security
Learning Center

CDSE
Center for Development
of Security Excellence

NTC
National Training
Center

NATIONAL SECURITY LEARNING CENTER INSTITUTIONS CONTINUE TO PROVIDE WORLD-CLASS TRAINING DURING COVID-19

By Adriene Brown and Colleen Coleman
Center for Development of Security Excellence (CDSE)

The National Security Learning Center (NSLC) is providing customer support during COVID-19, using existing learning technology to deliver world-class training through its institutions — the Center for Development of Security Excellence (CDSE) and the National Training Center (NTC).

CDSE's eLearning, case studies, security awareness games, and many more resources are available at www.CDSE.edu. Since the March 2020 stay-at-home orders have been in place, CDSE has seen a 44% increase in completed eLearning courses. These changes represent a 54% increase over the same period in 2019.

CDSE also quickly pivoted to bring the biennial Department of Defense (DoD) Security Conference online. The conference, originally planned as a hybrid event for DoD security professionals, took place virtually in late June with the theme "A Vision of the Future of Security" to address the department's priorities.

NTC just completed its first virtual Federal Law Enforcement Training Accreditation (FLETA) self-assessment. Three FLETA assessors reviewed the Investigations Case Analyst Program (ICAP) for reaccreditation, and ICAP was found to be in full compliance and ready for the official reaccreditation assessment in July. The official assessment will be among the first FLETA accreditation/reaccreditation assessments to be conducted entirely virtual. The process NTC used to create its electronic files for virtual assessment was named a "FLETA model practice."

NTC is actively working to make the best use of available For Official Use Only (FOUO)-approved technology to continue to deliver mission-critical training. Staff is assessing new ways to deliver in-person training in a virtual world, including some accredited programs. NTC is also looking at new processes, activities, and ways to deliver curriculum virtually while still maintaining its high level of quality training and continuing to meet accreditation standards. NTC is working on several initiatives, including conducting case analyst training via NTC Online and Microsoft Teams; creating NTC on-demand to support a broad range of training needs across Personnel Vetting; and conducting an online version of the Federal Background Investigator Training Program (FBITP) in phases via Microsoft Teams.

DCSA FINANCIAL MANAGEMENT TEAM WINS DOD AWARD

By Quinetta Budd
Office of Communications and Congressional Affairs (OCCA)

Members of the award winning OCFO team include:

DCSA:

Richard Bell
Kerry Dudley
Peter Frontin
Richard Hoffman
Kimilee Holt
David Johney
Valerie Johnson
Charlotte Jones
Meredith Morefield
Michelle Thomas

Defense Finance and Accounting Service (DFAS)

Charlene Anderson
Ryan Carlson
Ryan Cashdollar
Beth Gelfius
Maria Linn
Charlayne Martin
Michael Presley

Defense Logistics Agency (DLA)

Christopher Dedobbelaere
Sabrina Seals

Legacy NBIB

Timothy Miller

The DCSA Office of the Chief Financial Officer (OCFO) was recently named an Under Secretary of Defense (Comptroller) 2019 Financial Management Award winner, which recognizes significant contributions to financial management improvement. In 2019, the Financial Management Awards Program Board evaluated 79 nominations, and OCFO's Initialization and Operations Team was one of 16 winners.

The Initialization and Operations Team was recognized for its efforts transferring the National Background Investigations Bureau (NBIB) and the background and suitability investigation mission from the Office of Personnel Management (OPM) to DCSA. Realignment of the NBIB workload was accelerated into a 12-month timeline with operations to be completed by October 1, 2019.

“We were challenged not necessarily to expose our weaknesses but to discover our strengths and resilience to overcome all obstacles as a team,” said Acting Chief Financial Officer Dr. Cherry Wilcoxon, discussing how her team won the award. “We leaned not on our own knowledge but leveraged the skills and knowledge of our internal and external partners and many others.”

During the realignment of the workload, OCFO solved complex contract conversion issues, developed projections, and coordinated accounting activity of almost $1 billion in financial resources. The team transitioned more than 3,000 employees to a new timekeeping system and trained new payroll customer service representatives to assist those employees.

Since a Defense Working Capital Fund (WCF) hadn't been stood up in the DoD in over 20 years, the team also formulated requirements to implement the first full-scope WCF within the Defense Agencies Initiative (DAI) financial management system. DCSA's WCF was open for business in DAI as scheduled, without any breaks in customer service. To maintain a high level of customer care and relationship management, DCSA established a call center to oversee billing and collections, agreement management, reconciliations, and issue resolution.

As long-term technology capabilities are still under development, OCFO built an interim information technology solution to function as a bridge between the legacy NBIB case management system and DAI for processing billing and revenue events. These efforts provided the ability to streamline activities under one umbrella, enhancing policies, financial processes, case management functions, and technological capabilities. The end result was a continual decrease in the investigative case inventory from more than 400,000 to about 250,000 cases, thus strengthening the nation's security.

“The ultimate measure of this team was not where we stood in the moments of comfort and convenience,” Wilcoxon said, “but where we stood during the times of challenge and skepticism — we stood united!”

PITTSBURGH FEDERAL EXECUTIVE BOARD RECOGNIZES FINANCIAL MANAGEMENT, PERSONNEL VETTING TEAMS

During this year's Public Service Recognition Week, the Pittsburgh Federal Executive Board (FEB) named DCSA Financial Management the 2020 Excellence in Government Awards Silver Award winner in the Outstanding Team category. Personnel Vetting Quality Assurance also received an honorable mention in the Outstanding Team category.

The Pittsburgh FEB is comprised of more than 100 federal agencies and over 20,000 federal employees. It strives to provide effective communications and coordination between federal agencies as well as all levels of government. The FEB's goal is to be a constructive, unifying force within the federal government and community by facilitating valuable collaboration.

SILVER AWARD
OUTSTANDING TEAM

DCSA Financial Management, Boyers, Pennsylvania

Team Members:

Timothy Miller
Steven Anderson
Adam Watson
Jason McCloskey
Autumn Best
Rebecca Stebbins
Brian McCue
Katelyn Klingler
Lynne Barth

HONORABLE MENTION
OUTSTANDING TEAM

DCSA Personnel Vetting Quality Assurance, Boyers, Pennsylvania

Team Members:

Bruce Soule
Yvette Harrison
Mike Kraynik
David Igoe
Sandy Tebay

COMPANIES RECOGNIZED FOR EFFECTIVE CI PROGRAMS, ENHANCING NATIONAL SECURITY

By Stephen Smith
Counterintelligence Directorate

In March, the Defense Counterintelligence and Security Agency (DCSA) announced the winners of the DCSA Excellence in Counterintelligence (CI) Award for Fiscal Year 2019: Digital Receiver Technology, Inc., Extreme Engineering Solutions, Raytheon Technologies Corporation, Lockheed Martin Corporation, and the Texas A&M University System.

DCSA annually recognizes cleared companies exhibiting the most impressive counterintelligence capability and cooperation with U.S. government efforts to deter, detect, and disrupt the theft of sensitive or classified U.S. information and technology by foreign entities.

DCSA field personnel identify candidates for this award and they are formally nominated by a panel of DCSA counterintelligence region directors. After the nominations arrive at DCSA headquarters, a panel composed of senior leaders from across the enterprise conducts a three-stage selection process to identify winners based on the assessment of company-submitted CI and insider threat reports that specifically led to the opening of full field investigations, operations, or other activities by federal agencies. Other significant company actions that detected and countered foreign intelligence activities are also considered, including actions that led to disruptions, prosecutions, convictions, debarments, and administrative actions.

The Excellence in CI Award is intended to encourage highly mature and effective counterintelligence programs that enhance national security and promote the uncompromised delivery of sensitive and classified services and capabilities to the Department of Defense and other U.S. government agencies.

The following highlights each winner’s efforts and how they achieved excellence in counterintelligence.

DRT Digital Receiver Technology, Inc.

In 2019, Digital Receiver Technology, Inc. (DRT), a global communications and signals company, achieved a 100% referral rate for reports submitted to DCSA. In other words, 100% of DRT's suspicious contact reports (SCR) met the benchmark for referral to a federal investigative agency. This is a remarkable statistic and testimony to the attention to detail, quality, and completeness of DRT's exemplary reports.

One DRT SCR reported an individual posing as a U.S. government representative who placed a multi-million-dollar order for highly sensitive International Traffic in Arms (ITAR)-controlled Signals Intelligence (SIGINT) equipment. DCSA made a quick referral to Homeland Security Investigations and the Defense Criminal Investigative Service (DCIS) and a joint investigation was opened. The investigation identified several suspects involved in procurement fraud, as well as other criminal activities involving foreign entities and connections. As the initial investigation was winding its way through the investigative and legal process, DRT reported an inquiry from an individual who had recently purchased the contents of a storage container at an auction sale.

While going through his newly purchased property, the individual located DRT equipment, including SIGINT equipment. DRT personnel recognized a likely connection between this report and the ongoing criminal investigation and immediately notified DCSA. The investigation expanded, resulting in the recovery of millions of dollars of highly sensitive stolen SIGINT equipment subject to ITAR and export controls. Eight arrests were made, and another subject has an active warrant. In addition to the high value seizures of ITAR and export-controlled equipment, DRT's reporting essentially identified a new method of operation being used by criminals to illegally purchase and sell ITAR and export-controlled, military-use equipment to unauthorized entities and persons.

X-ES

Extreme Engineering Solutions (X-ES) — a leader in design and manufacturing of embedded computing solutions — operates supply chain and quality control risk management programs to ensure the parts used in their military products are always original parts, manufactured to exacting specifications for U.S. military applications. In 2019, X-ES's supply chain team detected and sidelined a counterfeit shipment of capacitors intended for vital military equipment. The company notified DCSA, removed the counterfeit parts, and the original supplier from the supply chain, as well as referring the matter to other government agencies.

In a recently concluded case going back to 2012, X-ES reported a suspicious foreign solicitation to purchase power supplies for man-portable air defense systems (MANPADS), night vision goggles, and other military equipment. The report resulted in a long-term undercover investigation by U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HIS) and the DCIS. In the course of the ensuing investigation, a foreign businessman was arrested, tried, and convicted for attempting to provide U.S. military equipment to a terrorist organization. The subject was sentenced to 10 years in prison. Had the shipment succeeded, the MANPADS, once operational, represented a direct threat to U.S. personnel flying with host-country personnel during air operations.

LOCKHEED MARTIN

Lockheed Martin Corporation (LM), a global security and aerospace company with a leading counterintelligence program, has now won this award five times. Lockheed Martin runs a highly diversified and agile program that evolves and advances to leverage new and improved technologies and capabilities to meet and respond to threats. Lockheed Martin's Insider Threat program continuously vets digital and human behavior of all 110,000 employees using a proprietary tool developed to detect suspicious activity and behavior. The company then conducts inquiries to assess what may or may not be occurring.

Lockheed Martin's CI program is a key component of the newly established Security Fusion Center, an apparatus developed to integrate key threat intelligence resources across the company's security and CI functions in a secure, centralized location. The center allows for quick and comprehensive analysis of a broad spectrum of CI concerns.

Lockheed Martin also leverages some of the most advanced insider threat tools in industry, such as a classified cybersecurity operation monitoring capability for classified networks, an advanced "Shark Cage" providing game-changing awareness into classified cyber behaviors and environments, as well as an asset and countermeasures tool that tracks national security and Lockheed Martin critical assets identified at each site.

Raytheon Technologies

Raytheon Technologies Corporation is an aerospace and defense company that provides advanced systems and services for commercial, military, and government customers worldwide. The company, formed in 2020 through a merger of Raytheon Company and the United Technologies Corporation, an aerospace business, is headquartered in Waltham, Massachusetts.

Raytheon Technologies recently embarked on a focused initiative to build one of the most advanced insider threat/CI capabilities in cleared industry to protect information, technology, personnel, and facilities from insider threats and foreign adversaries targeting sensitive and classified technology. The company's program provides actionable intelligence to DCSA, the Federal Bureau of Investigation (FBI) and other law enforcement, as well as the Intelligence Community (IC) to ensure the protection of U.S. technologies.

The Raytheon Technologies Insider Threat program achieved significant advancements in 2019. It achieved measurable results by enabling tighter data controls, enhanced data monitoring and behavioral analytics, an enterprise-wide educational campaign, and strong cooperation with DCSA, the IC, and industry partners. In 2019, the company's reporting resulted in a significant number of full-field federal investigations or operations, searches, and seizures of large amounts of digital media containing sensitive, proprietary, and ITAR/export-controlled information. Raytheon Technologies reporting was also published in several formally evaluated "high value" intelligence information reports (IIRs).

TEXAS A&M UNIVERSITY

Texas A&M University System is one of the nation's premier Tier 1 Research Universities. Texas A&M research, development, and education programs touch most, or all, of the technologies listed on the Industrial Base Technology List (IBTL). This is Texas A&M's second award.

In 2019, Texas A&M reporting led to over 100 referrals to other government agencies and a significant number of actions and activities to address threats to U.S. technology resident at Texas A&M.

Texas A&M is a leader in the academic community for counterintelligence and security. It sponsors and supports the annual four-day Academic Security and Counter Exploitation Conference for academic institutions across the country. The 2020 conference was attended by representatives from more than 80 universities, including over 50 cleared institutions. It featured presentations from DCSA, FBI, Department of Commerce, Department of State, and the IC. Texas A&M established the Academic and Security Counter Exploitation program, a forum for information sharing and benchmarking that facilitates securing of research portfolios at U.S. universities. The group now has more than 400 individual members. They also host a quarterly counterintelligence working group to partner with government agencies in protecting technology and research on the Texas A&M's 11 universities.

Texas A&M designed and deployed a NIST 800-171 compliant secure computing enclave to host all DoD and other federally sponsored research efforts. Texas A&M is also working with its congressional delegation to sponsor legislation that would provide a robust environment for protecting technology across the academic enterprise.

Cleared industry and cleared academia face a steady stream of malign foreign actors who are constantly adapting their methods of operation and methods of contact to get at national security information and technology. In response to the ever-changing threat, Texas A&M continuously responds with improvements to its CI program. In 2019, Texas A&M launched new tools and capabilities to identify emerging and asymmetric foreign threats to academic institutions with high success.

SEMINAR LINKS ACADEMIA WITH FEDERAL PARTNERS

By Demetric T. Tucker, DCSA Industrial Security Directorate (ISD)
Kevin R. Gamache, Texas A&M University System

In early March 2020, the Texas A&M University System hosted its fourth annual Academic Security and Counter Exploitation (ASCE) seminar on the Texas A&M University campus in College Station, Texas. The seminar brought together over 225 representatives from 75 universities from across the country and 16 government agencies to address security threat to the nation's academic research enterprise. Texas A&M established this forum in 2017 as a service to the academic community.

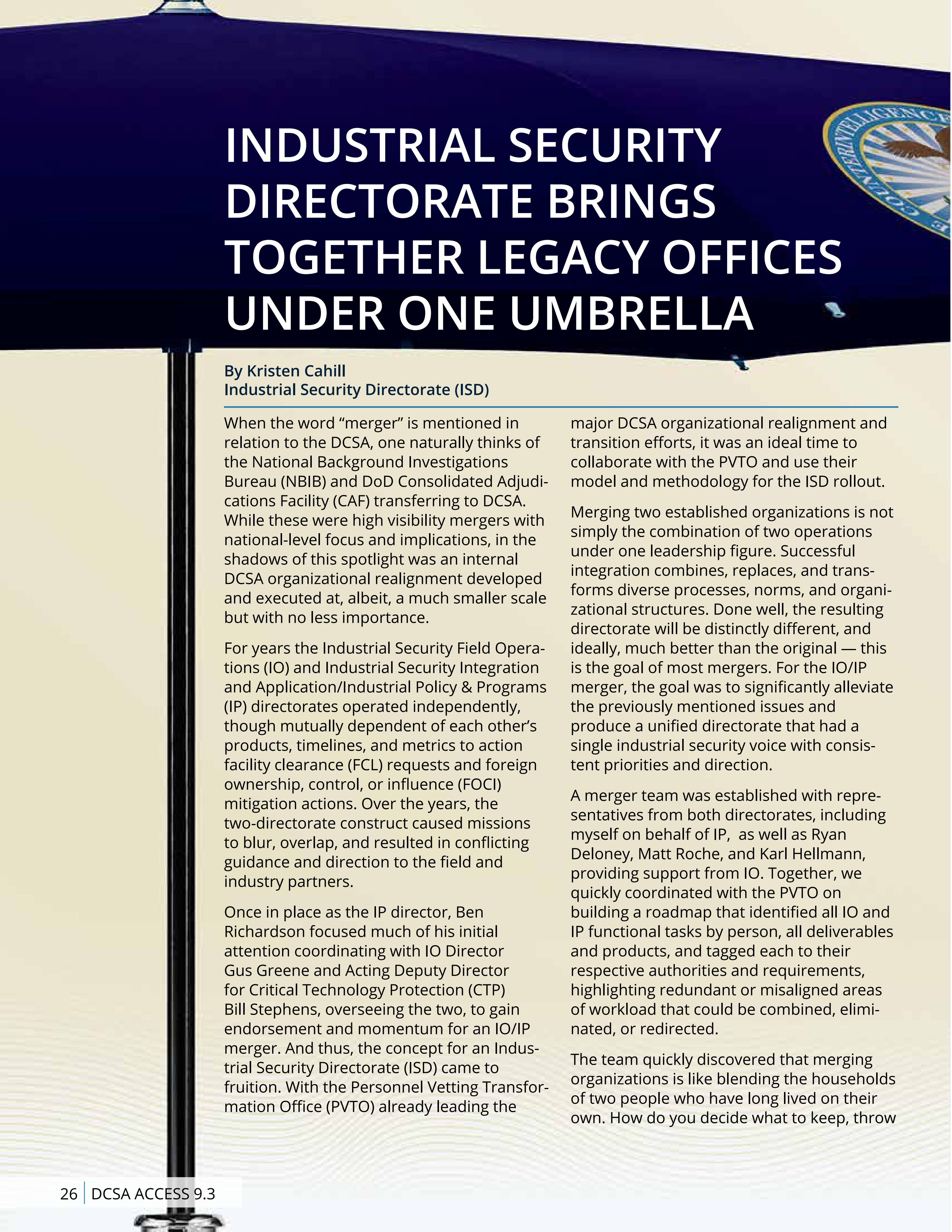
The ASCE mission is to increase awareness of threats posed by malign foreign actors to research and development conducted at U.S. research universities. The group provides tools for countering foreign influence, in coordination with federal law enforcement and intelligence agencies.

This year's seminar provided tracks for executive leaders, compliance and security officers, information security professionals, and federal officials to engage across a wide variety of topics. The seminar also featured a day and a half workshop focused solely on colleges and universities participating in the National Industrial Security Program (NISP).

The conference agenda featured national counterintelligence (CI) leaders who shared their unique perspective of the threat the United States is facing today. David Bowdich, deputy director of the Federal Bureau of Investigation (FBI), stressed the importance of the federal government's partnership with academia. Kelvin K. Droegemeier, director of the White House Office of Science and Technology Policy (OSTP), discussed current initiatives underway to strengthen America's research environment. Bill Evanina, director of the National Counterintelligence and Security Center (NCSC), provided insight into current counterintelligence challenges faced by academia. Finally, John Demers, assistant attorney general for national security, was joined by Michael K. Young, president of Texas A&M University, in a conversation focused on balancing national security with the open environment of academia.

While the conference was focused primarily on sharing threat information, the event also allowed participants to interact with leaders from DCSA. Mike Halter, deputy director of Industrial Security Directorate (ISD), provided tremendous insight into changes within DCSA. Leaders from DCSA also conducted an "Ask DCSA" panel discussion, which allowed participants to engage subject matter experts with issues of concern. Demetric Tucker, DCSA industrial security representative, joined by Ronald Wooten, CI special agent, shared best practices through collaborative workshops. Special Agents in Charge (SAC) Andy Rodriguez and Rolland Neve, from the Personnel Vetting San Antonio Field Office, and Robert Rodriguez, also a SAC from the Personnel Vetting Houston Field Office, provided an overview of the Personnel Vetting mission and common mistakes made on the Standard Form 86 (SF-86). Additionally, Heather Mardaga, deputy director of the Vetting Risk Operations Center (VROC), provided a status brief on Continuous Evaluation (CE). During the conference, Monica Clory, also from VROC, manned a kiosk that offered security professionals a real-time status review of their personnel security clearances.

The ASCE seminar continues to evolve and has already become one of the premier events of its kind, focused on protecting this nation's critical academic research infrastructure.



INDUSTRIAL SECURITY DIRECTORATE BRINGS TOGETHER LEGACY OFFICES UNDER ONE UMBRELLA

By Kristen Cahill
Industrial Security Directorate (ISD)

When the word “merger” is mentioned in relation to the DCSA, one naturally thinks of the National Background Investigations Bureau (NBIB) and DoD Consolidated Adjudications Facility (CAF) transferring to DCSA. While these were high visibility mergers with national-level focus and implications, in the shadows of this spotlight was an internal DCSA organizational realignment developed and executed at, albeit, a much smaller scale but with no less importance.

For years the Industrial Security Field Operations (IO) and Industrial Security Integration and Application/Industrial Policy & Programs (IP) directorates operated independently, though mutually dependent of each other’s products, timelines, and metrics to action facility clearance (FCL) requests and foreign ownership, control, or influence (FOCI) mitigation actions. Over the years, the two-directorate construct caused missions to blur, overlap, and resulted in conflicting guidance and direction to the field and industry partners.

Once in place as the IP director, Ben Richardson focused much of his initial attention coordinating with IO Director Gus Greene and Acting Deputy Director for Critical Technology Protection (CTP) Bill Stephens, overseeing the two, to gain endorsement and momentum for an IO/IP merger. And thus, the concept for an Industrial Security Directorate (ISD) came to fruition. With the Personnel Vetting Transformation Office (PVTO) already leading the major DCSA organizational realignment and transition efforts, it was an ideal time to collaborate with the PVTO and use their model and methodology for the ISD rollout.

Merging two established organizations is not simply the combination of two operations under one leadership figure. Successful integration combines, replaces, and transforms diverse processes, norms, and organizational structures. Done well, the resulting directorate will be distinctly different, and ideally, much better than the original — this is the goal of most mergers. For the IO/IP merger, the goal was to significantly alleviate the previously mentioned issues and produce a unified directorate that had a single industrial security voice with consistent priorities and direction.

A merger team was established with representatives from both directorates, including myself on behalf of IP, as well as Ryan Deloney, Matt Roche, and Karl Hellmann, providing support from IO. Together, we quickly coordinated with the PVTO on building a roadmap that identified all IO and IP functional tasks by person, all deliverables and products, and tagged each to their respective authorities and requirements, highlighting redundant or misaligned areas of workload that could be combined, eliminated, or redirected.

The team quickly discovered that merging organizations is like blending the households of two people who have long lived on their own. How do you decide what to keep, throw

out, share, or replace? Organizational integration is not just about prioritizing a list of projects. It's about deciding what capabilities will be retained, replaced, or consolidated, which was an inclusive and collaborative effort among our cross-functional team and directorate leadership.

After briefing senior directorate leaders on multiple occasions, the merger team presented its merger methodology to the PVTO. On February 12, after reviewing the data, the PVTO endorsed the implementation and the IO/IP merger became official. The merger team then went to work executing its phased approach, focusing on three major phases that centered on division and branch level realignments, aligning these phases to coincide with pay periods. While finalizing the phases, we realized that simply communicating was not enough to build buy-in for a post-merger integration. We needed a robust organizational change management and communications strategy to:

- Present a case for change and create a sense of urgency for necessity of the merger.
- Position the merger among other IO and IP strategic initiatives.
- Create a compelling vision for the new organization with clearly articulated benefits.
- Develop a steady drumbeat of key messages to IO/IP personnel to communicate progress and explain the "what's in it for me."

With this in mind, the merger team held multiple town halls, fielded questions and concerns, developed and distributed a merger slick sheet and all-hands emails, and engaged individually with personnel directly affected by the realignment. The merger was also included as a major fiscal year operational goal.

The objective was to ensure frequent and meaningful messaging was provided to the IO/IP workforce in regular intervals. Externally, the focus was to "first, do no harm" and not break anything providing valuable service to industry and government partners. This was successfully executed as stakeholders experienced no disruption in services.

From conception in December 2019 to initial operating capacity in April 2020, the Industrial Security Directorate, led by Gus Greene, was established. The newly aligned directorate has already proven to process faster facility clearances and FOCI mitigations and with better results, and the new directorate is more agile and responsive to changing conditions within cleared industry as a whole.

Achieving real alignment — in which strategy, goals, and meaningful purpose reinforce one another — gives any organization a major advantage. It provides a clearer sense of what to do at any given time and enables trust of people to move in the right direction. For ISD, the result was a new directorate that focused less on deciding how and what to do and more on simply doing. No restructuring is ever easy, but with a firm grasp of a few change management concepts, a structured approach, and guidance from established best practices, the process was less painful than anticipated and infinitely more rewarding.

AGENCY WELCOMES ITS FIRST CHIEF DATA OFFICER

Wally Coggins, a detailee from the Office of the Director of National Intelligence (ODNI), started his joint duty assignment as the DCSA Chief Data Officer (CDO) in early March with just enough time to prepare for telework in response to the COVID-19 pandemic. “This is my first experience in 30 years of government service teleworking,” he said. “However, I have been incredibly impressed by the dedication of the DCSA workforce during the health crisis, and despite HPCON CHARLIE status since mid-March, the ability of the agency to maintain such a high and effective operational tempo.”

Prior to joining DCSA, Coggins was the director of the Intelligence Community Security Coordination Center (IC SCC). The IC SCC is responsible for the integrated cyber defense of the IC information environment, covering all of the Top Secret (TS) and Sensitive Compartmented Information (SCI) networks and enclaves connected to Joint Worldwide Intelligence Communications System (JWICS).

Coggins explained that in order to accomplish the IC SCC’s mission, the center acquires, processes, analyzes, stores, and secures a very high volume of cybersecurity data, providing the tools, capabilities, and reporting to rapidly share situational awareness and coordinate incident response during major cyber events. “During that assignment, I gained a firsthand appreciation of the importance of effective data management practices and their importance to mission success,” said Coggins.

Coggins compared that experience with the needs of DCSA. “At its core, DCSA is a data driven organization, and there are enormous opportunities to improve mission effectiveness and enterprise-wide decision making through how we manage and leverage data as an agency asset,” he said. “Our goal is to lead the implementation of data management strategies, governance, and other initiatives that provide end users with high quality, timely, and actionable data to drive optimal mission and business outcomes.”

He added that maturing the agency’s data management capabilities is foundational to fostering innovation through increased automation and sophisticated analytics, and ultimately adopting advanced technologies including machine learning and artificial intelligence. “DCSA has incredibly important and highly relevant missions to advance and preserve America’s strategic edge. Each of these missions, and the corporate functions that support them, require timely, accurate, and complete data to do their jobs,” said Coggins.

According to Coggins, the CDO also has an important role increasing agency-wide data and analytic literacy to empower the workforce with the knowledge and skills to find new value in data assets. In order to accomplish these objectives, the CDO is responsible for developing the agency’s data strategy and roadmap, identifying capabilities and tools to govern and manage data, as well as establishing data standards, architectures, and performance measures.

Since his arrival, Coggins has started to build on the existing Enterprise Data Management (EDM) program that Michael Mitchell was developing as a strategic planning and integration initiative. For example, EDM has developed an agency data strategy and roadmap and is leading collaboration initiatives with the DoD Chief Data Officer, Chief Management Officer, and Chief Financial Officer to leverage department-level

data management tools and capabilities, while supporting a series of pilot projects to acquire open source data in partnership with Industrial Security Directorate (ISD) and Personnel Vetting (PV) stakeholders.

"With the recent creation of DCSA and the planned integration of additional components from the Defense Information Systems Agency (DISA) and Defense Intelligence Agency (DIA), our current focus is expanding the foundational data strategy, roadmap, and data management capabilities to cover the agency's expanded mission set and enable more effective use of data across the agency with our mission partners," he explained.

He added that these transfers represent a significant expansion of the agency's mission and increase in the volume, variety, and velocity of agency data. "This increases the complexity of the data management challenge," said Coggins. "However, it also provides enormous opportunities to gain new insights across the mission areas and at the enterprise level when we make the various data sets discoverable and accessible agency-wide."

Coggins gave an example: The same data that is acquired for Continuous Evaluation (CE) of cleared personnel may also be highly relevant to the insider threat, counterintelligence, and supply chain security missions. "At the same time, we are making the legacy data more accessible across the agency for innovative mission insights. We must ensure Personal Identifiable Information (PII), Personal Health Information (PHI), and other sensitive data are appropriately controlled and secured. These are just a few of the many complexities and opportunities for DCSA as we work to integrate the components and improve data management practices," he said.

The effort is not without its challenges, added Coggins. "Advancing data management at DCSA will require crosscutting initiatives involving not only technology, but human capital and process. We are a small team and the number of initiatives across the agency we can potentially get involved with is very large."

He said one of the biggest challenges is prioritizing which projects will best enable the agency to improve data management maturity, mission operations, and enterprise business decisions. In addition, he said, DCSA is the result of the merger of formerly independent lines of business that developed their own cultures and ways of doing things over time to successfully deliver their respective mission priorities. "Effectively integrating the newly formed agency and maturing data management practices of the components will require extensive communication and a highly collaborative approach to gain buy-in for enterprise-wide solutions," added Coggins.

"I want the workforce to know that the guiding principle of the CDO team is to relentlessly pursue and implement data management initiatives that empower DCSA personnel with higher quality and more timely data that results in improved mission outcomes and evidence-based business decisions," said Coggins in closing. "Our success is only realized when DCSA personnel are able to increase the mission value they derive from data and are able to successfully deliver on their operational objectives."

CONTINUOUS EVALUATION vs. CONTINUOUS VETTING

By Zaakia Bailey
Vetting Risk Operations Center (VROC)

Throughout the last year, DCSA has received questions about the Continuous Evaluation (CE) process, the Continuous Vetting (CV) model, and the difference between the two. The following guide is designed to provide a better understanding of the two programs and what they mean for the personnel vetting mission.

DCSA is meeting its timeliness goals for Top Secret investigations — 80 days — for the first time since Spring 2014. Secret investigations are averaging at 56 days. The investigative inventory remains under 200,000 cases.

Fact: CE and CV are not the same thing.

CE is a vetting process that reviews the background of individuals eligible to either access classified information or to work in a sensitive position. CE relies on automated record checks and business rules to continually assess an individual's eligibility. CE is one component of the greater Continuous Vetting efforts.

Per Executive Order 13764, CE will evolve into the CV model to support personnel security clearance (PCL) reform efforts. CV is a more robust, real-time review of a person's background to determine if an individual continues to meet applicable requirements. CV is a combination of automated records checks, self-reporting, agency specific reporting, insider threat reporting, and other analytical processes that are executed continuously to determine if a cleared person can remain a trusted insider.

It is expected that CV will replace the current practice of five and 10-year periodic reinvestigations (PR) with ongoing, and often automated, determinations of a person's security risk.

Fact: CE has not replaced periodic reinvestigations.

In accordance with January 2017 guidance, individuals are still required to submit a completed Standard Form 86 (SF-86) when a reinvestigation is requested. That happens at six years from the date of last investigation for Top Secret Tier 5 Reinvestigations (T5Rs) and at 10 years for Secret Tier 3 Reinvestigations (T3Rs). In June 2018, the Director of National Intelligence (DNI), and the Director of the Office of Personnel Management (OPM), jointly issued a memorandum establishing interim measures intended to mitigate the existing inventory of personnel security investigations at the National Background Investigations Bureau (NBIB). These measures included deferring reinvestigations when initial screening results are favorable and mitigation activities are in place. Agencies are permitted to screen new reinvestigation requests using a risk management-based approach by analyzing the SF-86 according to deferment protocol(s). The case is then either enrolled in CE or submitted to an investigation service provider (ISP) for reinvestigation.

Fact: CE will not result in more clearances being removed due to increased incident reports.

CE is a mechanism to identify unreported information that most likely should have been self-reported to a security manager. Nevertheless, the goal of CE is to address potential risk indicators as early as possible, allow subjects the opportunity to seek assistance, and mitigate the issue to a successful conclusion. When a CE alert is received, an analyst reviews it for validity and immediately triages the incident. Many incident reports are closed out within a matter of days. For those incidents that require further investigation or adjudication, additional reviews of the case are required but ultimately the intent is to mitigate the issue — not to revoke a clearance.

Fact: It is possible to verify whether an individual is enrolled in CE.

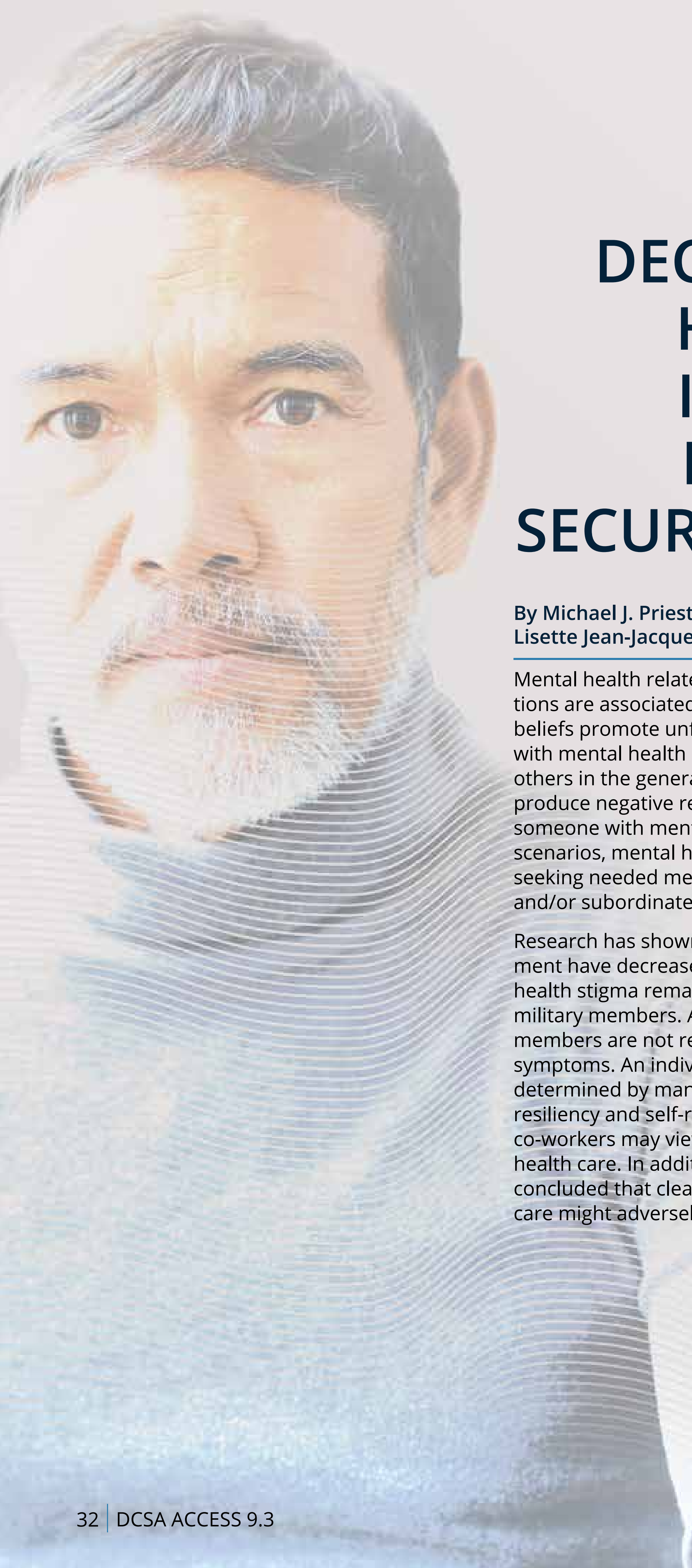
Department of Defense (DoD) CE enrollment history records are visible in the Defense Information Security System (DISS). Any DISS user with general access can view this information on a subject's summary page. The CE enrollment history includes the CE enrollment reason code and the date of enrollment or disenrollment in the CE program. If an individual is not enrolled, the summary will remain blank and state, "No records found." CE enrollment information is also visible in the Central Verification System (CVS).

Fact: Not all contractor under the National Industrial Security Program (NISP) are currently enrolled in CE.

All individuals with a DoD affiliation, eligibility for access, and a signed SF-86 dated 2010 or later are eligible for CE enrollment. As it currently stands, the cleared industry population accounts for 27% of the 2.1 million individuals enrolled in CE. DoD has set a goal to enroll all cleared DoD and NISP contractor personnel by the end of 2021.

Fact: Once a subject is enrolled into CE, incidents still need to be reported.

Employees are responsible for self-reporting adverse information concerning both themselves and other cleared employees. Even after an employee is successfully enrolled into CE, the security manager or facility security officer (FSO) should continue to report adverse information as a parallel and supporting effort to CE's automated records checks.



WORKING TO DECREASE MENTAL HEALTH STIGMA IN RELATION TO MAINTAINING A SECURITY CLEARANCE

By Michael J. Priester, PhD., Chief Psychologist, DoD CAF
Lisette Jean-Jacques, Psy.D., Staff Psychologist, DoD CAF

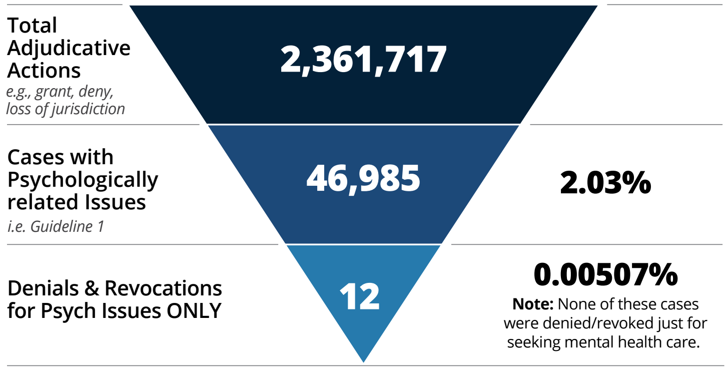
Mental health related stigma is the belief that mental health conditions are associated with adverse qualities and behaviors. These beliefs promote unfair stereotypes, such as the idea that individuals with mental health conditions are inherently more dangerous than others in the general population. Mental health stigma can also produce negative reactions in either the requester or others if someone with mental health symptoms seeks care. In worst case scenarios, mental health stigma actually stops individuals from seeking needed mental health care or from supporting a co-worker and/or subordinate who seeks help.

Research has shown that stigmas related to mental health treatment have decreased during recent years. Nonetheless, mental health stigma remains a problem. That's notably the case among military members. A 2014 RAND study showed many service members are not regularly seeking needed care for mental health symptoms. An individual's reluctance to seek mental health care is determined by many factors, including personal beliefs about their resiliency and self-reliance, beliefs about how their supervisors and co-workers may view their decision, and the availability of mental health care. In addition, the RAND study clearly and repeatedly concluded that cleared individuals fear that seeking mental health care might adversely impact their security clearance eligibility.

Why focus on decreasing mental health stigma among the cleared workforce?

Denial and Revocation Rates: Facts

DoD CAF Metrcis: 2012-2018



Bottom line: It is extremely rare for someone to lose a clearance for a psych issue alone.

If a cleared individual does not seek appropriate care when they experience mental health symptoms, there are many possible negative outcomes:

- **Decreased force readiness**: Mental health issues are common. Up to 30% of American adults experiencing mental health problems annually. If proper care is not sought, it can impact a cleared individual's ability to deploy or perform their job, including sensitive national security tasks. Mental health problems often occur with, and can increase, other physical health issues.
- **Increased suicide risks**: According to the 2018 DoD Annual Suicide Report, suicide rates by military members are rising. Nearly half of those committing suicide received Military Health System (MHS) care in the 90 days prior to death.
- **Increased security concerns:** Having an untreated psychological condition increases the risk that an individual will perform sensitive national security duties while overly burdened by emotional issues.

The DCSA's Personnel Vetting employees are addressing medical health-related concerns among workers who hold clearances. The Department of Defense Consolidated Adjudications Facility (DoD CAF) adjudicators and psychologists are exploring clearance eligibility concerns related to cleared individuals who seek mental health care to help destigmatize mental health concerns. According to DoD CAF Acting Director Marianna Martineau, "The DoD CAF encourages the cleared workforce to seek appropriate mental health care when necessary."

Despite the widely held belief, a detailed analysis of denial and revocation statistics involving psychological conditions clearly demonstrates that a cleared individual is not likely to lose or fail to gain clearance eligibility after seeking seek mental health care or experiencing mental health symptoms. From 2012 to 2018, the DoD CAF rendered 2.3 million adjudicative actions, including those granting or denying clearance eligibility or determining jurisdiction. Among these actions, only 2% involved psychological-related concerns. Of those, only 12 individuals had their clearance eligibility revoked or denied solely for security concerns presented by a psychological condition. That amounts to less than 0.0005% of all clearance actions.

Even for individuals with concerns in other adjudicative areas, the loss or failure to gain clearance eligibility was rare. During that same period, only 380 individuals with psychological concerns in addition to one or more other concerns had their eligibility revoked or denied. Of particular note, none of the cases resulting in a denial or revocation were based solely on an individual seeking mental health care. Rather, other factors, such as non-adherence to medical recommendations or simply not seeking care in the face of a clear need for mental health support, were generally the disqualifying issues.

Seeking mental health care is one of the most common ways that psychological concerns are addressed during the personnel vetting process. To educate people on these findings, DoD CAF psychologists developed a presentation illustrating the low likelihood that a cleared individual will lose or fail to gain clearance eligibility due to a psychological condition. By sharing these presentations with the cleared workforce, DoD CAF psychologists will continue to encourage seeking effective and needed support for emotional concerns.

LOOKING OVER THE HORIZON TO DISS

By Chuck Tench
Defense Vetting Directorate (DVD)

Users of the Joint Personnel Adjudication System (JPAS) are now transitioning to the Defense Information System for Security (DISS). JPAS was developed more than two decades ago as the DoD system of record (SOR) for recording clearance eligibility determinations and determinations of access to classified information up to Top Secret. Consisting of two modules, JPAS supported security managers with the Joint Clearance Adjudication Verification System (JCAVS) and adjudicators via the Joint Adjudication Management System (JAMS).

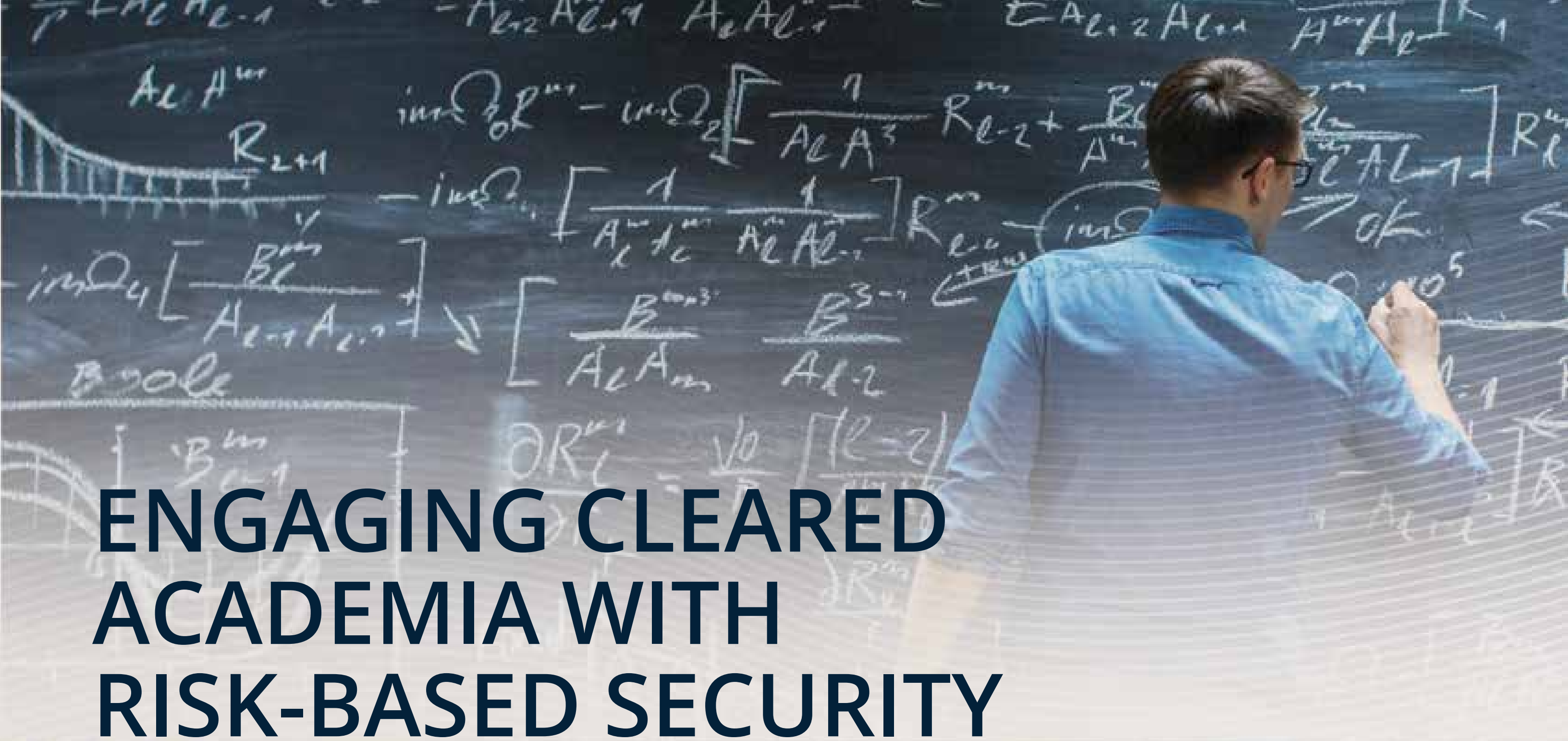
Transitioning to DISS provides numerous enhancements over JPAS, including better visibility of case inventory, electronic processing of SF-312s (classified information nondisclosure agreements), enhanced ability to securely submit and receive supporting documents, and better integrated workflows between adjudicators and security management offices.

When DISS is fully operational later this year, JPAS will be decommissioned and DISS will serve as the SOR for comprehensive personnel security, suitability, and credential eligibility management for all military, civilian, and DoD contractor personnel. DISS also provides secure communication between adjudicators, security officers, and component adjudicators in support of eligibility and access management.

DISS consists of two applications: the Joint Verification System (JVS) and the Case Adjudication Tracking System (CATS). These applications replace JCAVS and JAMS, respectively, providing enhanced benefits to the personnel vetting process.

JVS is designed to support DoD security officers, facility security officers (FSO) in industry, human resource managers, and component adjudicators in verifying eligibility, recording access determinations, submitting incident reports and visit requests, and communicating with the adjudicators.

DCSA will continue engaging user groups to seamlessly transition from JPAS to DISS, while addressing technical enhancements and process improvements as the agency begins to transition to the National Background Investigative Services (NBIS).



ENGAGING CLEARED ACADEMIA WITH RISK-BASED SECURITY

By Michael Rudzinski
Phoenix Field Office

As a DCSA industrial security representative, working with a cleared university can seem daunting. Its organization is unique, the openness of the university environment appears contrary to good security measures, and sometimes university leadership seem to be less supportive of the DCSA security mission than that of other cleared facilities. Regardless, cleared academia is critical to the Defense Industrial Base (DIB), as they are often the start of new technology discoveries, and they need to protect their critical proprietary information, as well as the government's national security information.

The role and scope of university research and its importance to national security

Universities have a three-fold mission: teaching, research, and public service. Universities and related academic organizations are at the forefront of innovation in the development of emerging technologies in every research discipline.

In Fiscal Year (FY) 2017, the Department of Defense (DoD) spent $5.6 billion for research and development (R&D) at 455 U.S. universities, with 96% of that total in the sciences, mathematics, and engineering sectors, primarily for unclassified research. Of these 455 academic institutions, 130 are cleared facilities, and they received nearly half of all federal R&D funding and 81% of the DoD funding for engineering R&D.

Continues on next page.

University structure and culture

The basic structure and staffing of a university are like that of a corporation, but with different or unusual names for structures. The table below illustrates some of the similarities and differences between the two types of organizations:

	CORPORATION	UNIVERSITY
Governing Board Members	Directors	Trustees, Regents, Governors, Fellows, Curators, Overseers, Visitors, etc.
Executive Officers	President, Chief Executive Officer, Chief Financial Officer, Manager	President/Chancellor, Chancellor/Provost, Comptroller, Dean, Director, Chair, Head
Subcomponent and Affiliated Organizations	Subsidiary, Branch, Division, Business Unit, Joint Venture, etc.	Campus, College, School, Institute, Center, Department, Auxiliary, Foundation, Non-Profit Corporation, etc.
Staffing	Salaried & Hourly Employees, Consultants, and Contractors.	Tenured & Non-Tenured Faculty & Academics, Civil Service Staff, Contract Employees, Graduate Teaching and Research Assistants, Undergraduate Assistants, Consultants & Contractors

Though corporations and universities are similar in organization, the culture of each is different. For example, corporations exist to make a profit, while universities are predominantly not-for-profit. The academic culture found at a university is defined by three unique concepts:

- **Academic Freedom:** Open inquiry and free expression in teaching, speaking, writing, and research by faculty and, to some degree, students is not to be restricted or punished.
- **Tenure:** This is permanent employment for faculty that protects them from retaliation for exercising academic freedom in their activities. Faculty earn tenure through a combination of teaching, research, and public service.
- **Shared Governance:** Faculty, staff, and students have a voice in governance mechanisms and decisions on matters which affect academic activities. Usually there are faculty and student bodies that have authority to make or join in decisions affecting academic matters. Faculty, students, and other academic staff can also serve as officers, governing board members, and participate in institution committees.

- **Other:** Other aspects of academic culture include diversity, inclusiveness, consensus, openness, and freely sharing university discoveries and knowledge with academic colleagues to foster academic inquiry and the general improvement of humankind as a collective whole.

Threats to academic research

An aggressive foreign espionage threat, which targets emerging critical technologies in U.S. academia, operates freely in the academic environment, including university facilities that participate in the National Industrial Security Program (NISP). While our adversaries target classified information and programs, they also seek unclassified information and proprietary research in critical emerging technologies that could be used to spur technology development and leapfrog the advancements in their homelands. Our adversaries usually employ, induce, or coerce a large number of foreign students, faculty, and visiting scholars — non-traditional collectors — and use a number of methods to acquire critical research from academia on American campuses. Academic culture's global, collaborative, and open nature creates a permissive environment for adversaries to target and acquire new discoveries and technologies with little risk.

Open collaboration between academics in the U.S. and abroad does not necessarily support a security culture that protects national security information. Universities are often skeptical of security requirements and compliance overreach because they are concerned that they could threaten academic freedom, fundamental research, and shared governance. Associating foreign students and scholars with espionage also alarms some academics as they believe this association may impair their international engagements with the "best of the best" and hinder university income streams from foreign sources. Finally, some faculty, staff, and students can agitate against university involvement with DoD and the federal government. Universities often find themselves caught in a struggle between university activists and government personnel over required security controls of U.S. sponsored research programs.

Challenges for classified (restricted) research in a university

There are also other challenges confronting classified university research. The first of these is compliance fatigue. While security professionals understand that security programs are put in place to protect national security, many university administrators and faculty often see security controls as just more compliance overreach. Universities maintain extensive compliance regimes to support research, including export control, human subject protection protocols, lab animal welfare, radiological and chemical safety programs, research integrity, and conflict of interest/conflict of commitment management, etc. Top tier research universities are audited extensively because they have a large portfolio of federal grants and awards. It's not unusual for them to have multiple federal audits at the same time. This compliance burden can trigger behaviors which do not support a close relationship between DCSA and the university and result in minimal cooperation from administrators and extensive oversight from the university's general counsel.

Another challenge facing university security programs is the issue of politics. Universities have a diverse set of stakeholders to whom they are accountable. Competing stakeholder agendas set the political debate at universities. While universities generally want to do applied or restricted information research, they do not want the political costs from those who think this type of research is a threat to academic freedom and shared governance or who just have a political bias against government-sponsored research. Classified research also has the appearance of restricting publication of research results, which can appear as a threat to academic freedom and the granting of faculty tenure. Even without a foreign espionage threat, these challenges can be a formidable obstacle to establishing good research security programs.

Strategies and best practices for engaging cleared academia

Given the importance of university research for national security and the issues with complex legal structures, academic culture, foreign espionage, compliance costs, and politics, what can DCSA personnel do to achieve superior security programs in cleared academia?

- **Establish a collaborative relationship with the security staff, researchers, and administrators:** Collaboration is an attribute of academic culture. Partner with university administrators and staff to develop a good security program that advances the interests of the university, faculty, staff, and students. If you identify an issue, have a suggested solution or mitigation with costs and benefits. Always identify the benefit to the university so they can exercise their shared governance of good security and risk mitigation.
- **Know your university:** Take the time to understand the structure of your university, know where classified research is conducted, identify the threat vectors, and understand who has the authority to enact changes. If you are uncertain, contact a university insider, start with the facility security officer (FSO), and ask them to explain or assist you.
- **Always be sensitive to the politics surrounding the university and to your potential impact on the key academic concepts:** academic freedom, tenure, and shared governance: Subscribe to the campus newsfeed. Read articles about espionage and export control incidents at universities. Know the university chain of command. Do not drop in unannounced on the university president or senior administrator without following the "chain of command" protocol. Let the FSO and administrators work approvals through the bureaucracy, even though it takes time.
- **Identify and work with academic "champions":** Work with the FSO to identify allies and supporters of government-sponsored research to help you and the FSO shepherd security program improvements that are outside the authority of the FSO. Get to know the export control officer too as they are a valuable source of information regarding violations, incidents, and sensitive programs that are likely related to national security.
- **Enable your FSO:** Educate your FSO and ask questions of things you do not understand. Point them to peer resources. Texas A&M University, for instance, has an Academic Counter Exploitation Newsletter and an FSO and Export Control listserv, both of which are available for university FSO/EO personnel. If there are other cleared academic facilities, consider creating a consortium or lunch group that meets regularly to educate academic security personnel on threats and share best practices of their institutions, like the Arizona Cleared Academic Contractors Conference (ACACC).
- **Know how to professionally address concerns, fears, or challenges to our security mission:** These are usually presented as threats to academic freedom, shared governance, tenure, and/or international collaborations. Have an "elevator pitch" to quickly and efficiently strip the anxiety or issue from impeding security. Always remind university personnel of our shared interest in protecting the faculty and student research that fosters scholarly activities and the transfer of university technology to the government and society, which remains under the control of, and for the benefit of, the university community.

The way forward

Working with universities and classified research programs can be challenging, but also very rewarding. Universities are leading the way in innovation and emerging technologies and they have a critical role in supporting our nation's warfighters. The effort you make today to improve university security programs will have a significant and long-lasting impact on protecting our national security.

Defense Counterintelligence and Security Agency

IRVING FIELD OFFICE CO-HOSTS OPEN HOUSE WITH PERSONNEL VETTING TEAM

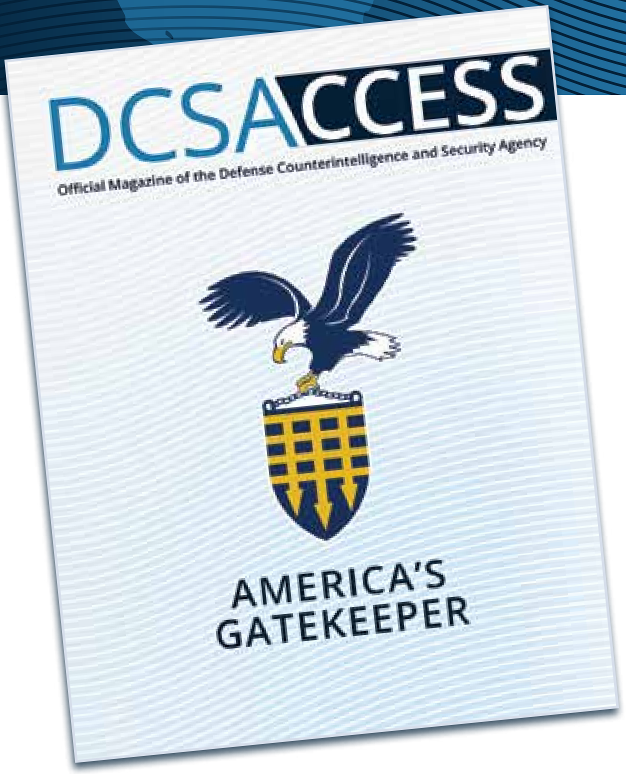
By Jennifer Norden
Irving Field Office Chief

The Irving Field Office co-hosted an open house in March, continuing the "One Team" campaign to introduce personnel from legacy National Background Investigations Bureau (NBIB) to those from legacy Defense Security Service (DSS) in the Dallas and Fort Worth areas in Texas.

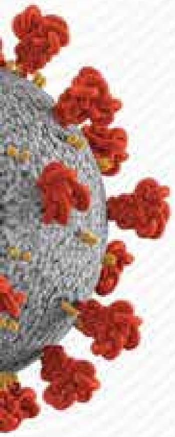
Personnel Vetting (PV) Special Agent in Charge (SAC) Lilly Cranor, Fort Worth area of responsibility, initiated this effort in December 2019 when she invited the Southern Region leadership to her monthly staff meeting. The approximately 35 DCSA attendees represented the various functional field elements: Investigators, industrial security representatives (ISR), information systems security professionals (ISSP), and counterintelligence (CI) special agents. Area Chief Robert Dubek and West Texas SAC James Couch were also in attendance. Norden and Cranor described their roles and daily work environment for their respective disciplines, while Dubek described the potential opportunities and gaps in our national security mission through the merged DCSA resources.

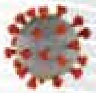
A mix and mingle allowed time for the agents and field office teams to get to further know each other. Afterward, the respective field office teams conducted their normal monthly staff meetings as separate breakout sessions. Dubek was able to attend a portion of the industrial security meeting and was introduced to the Vetting Risk Operations Center (VROC) team that supports the Irving Field Office. The engagement provided a front-line view of the internal coordination within the Industrial Security Directorate (ISD). The Irving Field Office will host similar events with the other Dallas and West Texas Personnel Vetting teams once COVID-19 circumstances allow.

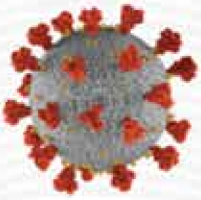
OCTOBER'S ISSUE WILL FEATURE IN-DEPTH COVERAGE OF THE AGENCY'S MISSION AREAS.


DCSACCESS
Official Magazine of the Defense Counterintelligence and Security Agency
AMERICA'S GATEKEEPER

STAY TUNED







DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

27130 Telegraph Road
Quantico, Virginia, 22134

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

www.dcsa.mil