Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper

Volume 3, Issue 4

Transfer of Authority

IN THIS ISSUE

IN THIS ISSUE

Vol 3 | ISSUE 4

DCSA Gatekeeper

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

FROM THE DIRECTOR

Editor's Note: This page normally features a message from the Director on the magazine's content, his priorities or key messages. Prior to his departure on Sept. 28, 2023, outgoing Director William K. Lietzau, sat down for an interview with staff of the Office of Communications and Congressional Affairs (OCCA) to share his final thoughts on the agency he led since March of 2020.

OCCA: You came to DCSA from the Personnel Vetting Transformation Office (PVTO), so you were familiar with the agency and the transfer of missions. What was your biggest surprise when you arrived as director?

Director Lietzau: When you look at the name Personnel Vetting Transformation Office, one could have assumed that all anyone cared about was personnel security and that personnel security needed to be upgraded. Then you say, why do you have the industrial security and the counterintelligence pieces? This led to one of my biggest surprises -- comprehending the importance of the mission of the entire agency and how it was much bigger than simply getting people more quickly through the personnel vetting process.

If you look at where we were in 2019 when I got involved in personnel vetting transformation, all people cared about was getting the backlog down and fixing the timeliness. We wanted people to get their clearances more quickly and it's a much more complicated mission than that.

Former DCSA Director William K. Lietzau responds to a question on continuous vetting during a roundtable interview with the Pentagon Press Corps in October 2021. (DOD photo by Christopher P. Gillis)

We have a changing environment with threats from our adversaries directed at our cleared workforce. At the same time, we have to maintain the quality of our background investigations and our adjudications in a changing culture.

Then you shift over to the industrial security side of the house and it gets even more complicated. You have an adversary that for years has been learning how to better influence corporate America and the industrial base of this country. And frankly from a national perspective, we've been focused on just that one small aspect that was associated with the move when we formed DCSA.

One of the biggest surprises was that the importance of the mission is so much greater than I ever thought. As a result, I learned that we needed to really work on what the agency needed to be to meet these challenges. That list was much longer and more significant than I would have thought. As if forming a new agency wasn't challenging enough, I became the Director just as the country entered the COVID lockdown.

OCCA: How did COVID affect your early decisions and did it limit how you implemented your vision for the agency?

Director Lietzau: It was difficult on that first day. I was about to say I shook hands with Charlie Phalen as we changed over directorship. But no, we weren't allowed to shake hands back then. We were touching elbows. And I looked at a camera lens and for the next few weeks I seemed to be the only person in the building and I would wander around wondering, do we really have all those employees out there that I'm told are on the other end of this camera lens? So clearly it was challenging and it changed the way we would do things.

I did have to alter plans because of COVID but would

I say it really impacted our operations in a negative way though? No, I don't think so. There was something about this agency that was prepared for change. We had just come through a transfer; we made sure everyone was getting paid and we tried to have as little turmoil as possible. That's the benefit of a seasoned professional like Charlie Phalen as the director, he brought a sense of calm to the agency. At the same time, everyone was poised knowing we're going to transform. That's why we were brought together. We weren't brought together just so we could make a couple agencies into one. We were brought together so that we could really become what America needed. So, everyone was poised for that. COVID became another thing that we had to adjust to.

You asked an earlier question about things that surprised me - I've talked about it frequently and that is just the quality and the character of our employees. That blew me away as I met them, and I've been in many different jobs and many different sets of employees. None surpasses what I saw at DCSA, but in looking at that, those employees took the COVID situation and leveraged it to do great things. Our security training people found a way to do online classes with greater skill than they had ever done it before, and certainly in greater numbers.

There is a picture of a room at Boyers, down in the mine, full of file cabinets and there's a picture post COVID with no file cabinets as we moved everything into electronic transmission capabilities. So, we leveraged COVID and I don't think we missed too many beats and I think that's a testament to the workforce that really was focused on that mission. There are always outside things that are going to change how you do your business, they're going to change your plan. You can put a plan of action with milestones and things in place, and you can try to achieve them on schedule. But if you're not ready to be flexible and move when something impedes your efforts, you're going to fail eventually. This agency did not fail. COVID didn't get in our way.

OCCA: Now that we're in this post COVID world, what would you say was your biggest challenge as director?

Director Lietzau: I think again, it's always hard when you say biggest challenge as there were so many. I often think about getting a common culture where people weren't identifying with their former organizations, or getting the regional structure in place, which was much harder to do with COVID. That was one of the things we had to delay a little bit.

There are still a lot of things that need to be fixed, but I guess one of the biggest ones was the fact that there wasn't a lot of attention on industrial security and what

James Shope (left, who recently retired), Background Investigations, and Jennifer Phillips, National Background Investigation Services, provide Lietzau with a tour of the Boyers Iron Mountain facility in June 2021. (DOD photos by Christopher P. Gillis)

At the end of the Change of Directorship ceremony in March 2020, Lietzau (right) and former Director Charlie Phalen hit elbows vice shaking hands as the COVID pandemic is in its early stages.

changes needed to be made to match an emerging threat, as we shift from counterterrorism to great power competition in the world. I had come up with the PVTO, but maybe they should have called it the security organization transformation office because it really needed to be bigger than looking it at from a personnel vetting perspective. All those things were big challenges but the biggest one I would say was how to prioritize what to do first. We had so many different things to do. In any organizational change, you need to do lots of things and you've always got long poles in the tent, like the finance side when you merge information technology, and getting your policies and procedures aligned. But when you have so many things to do and you have a quickly moving adversary, prioritizing what's the most important thing that you need to put first and sequencing all of those other things is one of the most difficult issues to deal with.

OCCA: Very early in your tenure as director, we heard you repeatedly mentioned that we are transferring, transitioning and transforming. Where do you think DCSA is in that process?

Director Lietzau: That's a great question and perhaps that to some degree attends my departure from the stage. I would say we're at the end of that at least with respect to what's necessary for the big merger that took place in 2019 and then some subsequent actions in 2020 and 2021. There's always going to be transformation of this agency. There has to be in order for this agency to meet the national security needs that the country has for us. But that transfer, transition, transformation alliteration is just kind of a nice way to package a sequence that gets us from different disparate organizations into one unified organization that's doing what the country needed it to do. And so we kind of finished transfer each time a transfer took place.

And I'm excited about coming back someday and saying, yes, I played a role before they were this great. They're already great, but we're going to be greater. I'm very confident of that.

In June 2021, Helena Brown (left), Industrial Security Directorate, passes a James S. Cogswell Industrial Security Award certificate to Lietzau (center), while Matt Redding, Assistant Director for Industrial Security, looks on.

Lietzau speaks at a townhall in June 2020 during the COVID pandemic. (DOD photos by Christopher P. Gillis)

Ceremony honors work of departing Director Lietzau; ushers in leadership of Acting Director Lecce

On Sept. 28, the Defense Counterintelligence and Security Agency (DCSA) bid farewell to its first permanent director, William K. Lietzau.

Lietzau began his tenure in March 2020 and was fond of recounting the ceremony acknowledging his appointment in a conference room with just a few people as employees watched remotely, adjusting to new life under COVID. Lietzau's farewell was much more in keeping with tradition and provided the pomp and circumstance missing at the former event. Held at the National Museum of the Marine Corps, the event featured the Quantico Marine Corps Base Ceremonial Band and Honor Guard and a formal Transfer of Authority.

John Dixson, Director for Defense Intelligence (Counterintelligence, Law Enforcement and Security), reflected on Lietzau's start at DCSA and heralded the agency workforce and its dedication to mission that helped Lietzau navigate DCSA through an era of extreme change. In fact, said Dixson, Lietzau's entire tenure was marked by change and transformation adding that DCSA has a no-fail mission and under Lietzau's leadership, continued to succeed and excel. In closing, Dixson said he was looking forward to DCSA's continued success.

John Dixson, Director for Defense Intelligence (Counterintelligence, Law Enforcement and Security), reflected on Lietzau's start at DCSA and listed accomplishments from Lietzau's tenure. (DOD photos by Christopher P. Gillis)

The Transfer of Authority included reading the appointment letter of Deputy Director Daniel Lecce as Acting Director and the passing of the DCSA flag from Lietzau to Lecce.

In his remarks, Lecce also lauded Lietzau's leadership and how he molded a workforce that came from disparate pieces into DCSA. He also cited Lietzau's investment in the workforce and how he treated employees with respect and empathy. Speaking to agency employees, Lecce said nothing gets done without the gritty dedication of the DCSA workforce and what he called the 'spirit of a Gatekeeper.' He promised to continue the great work of the agency.

Following the presentation of a retirement certificate and several gifts, Lietzau centered his remarks on thanking those who made the day possible, from the planning committee to his colleagues, mentors and most of all, his family. After recognizing each, Lietzau then directed his remarks to the men and women of DCSA. He described the workforce's selflessness, commitment to mission

Acting DCSA Director Daniel Lecce praised Lietzau's leadership and noted that he molded a workforce that came from disparate pieces into DCSA, during his remarks.

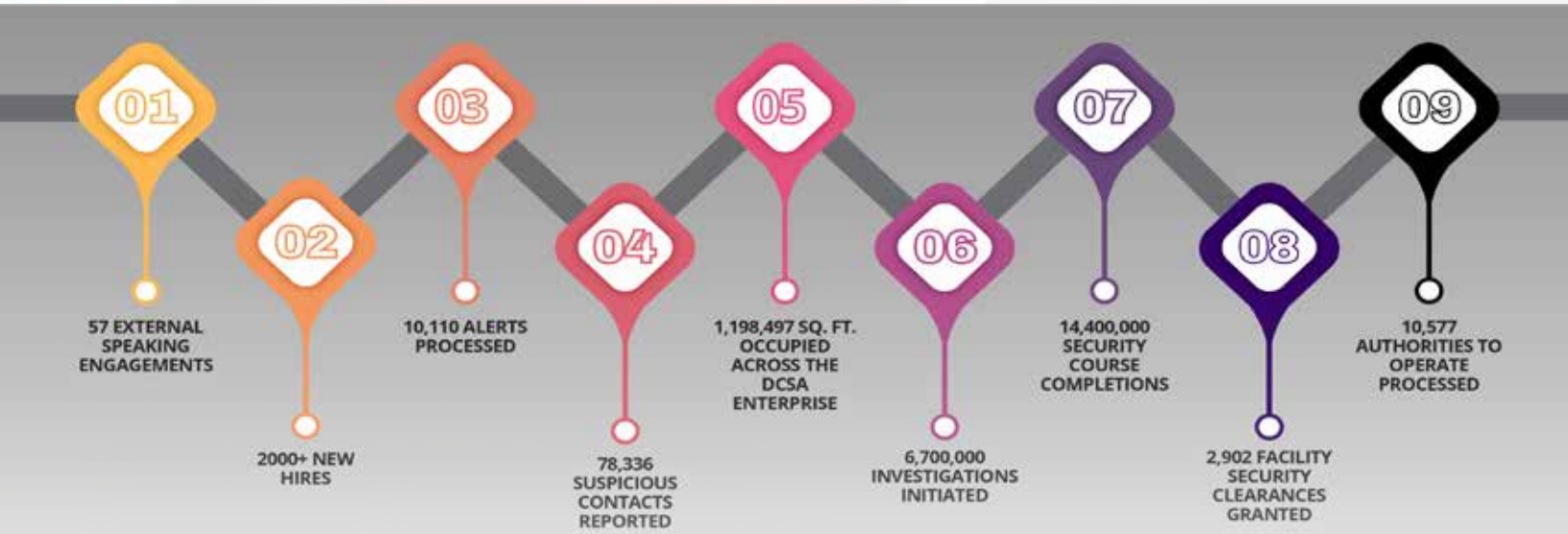
Senior leaders and agency employees watch the Transfer of Authority ceremony at the U.S. Museum of the Marine Corps. (DOD photos by Christopher P. Gillis)

During the Transfer of Authority portion of the ceremony, Lietzau (left) passes the DCSA flag to Lecce (right), while Chief of Staff Ellen Ardrey looks on.

and dedication. "It's very gratifying to have you as my colleagues," he said. In fact, he said it was the spirit and culture that attracted him to the agency.

During this tenure Lietzau also frequently quoted Alexander Pope, who said 'Act well your part. There all honor lies.' "This was my part," said Lietzau, "to have been the Director of DCSA at this time. I used to describe DCSA's transformation as building the jet while also flying it. You have built that jet and I could not be prouder of what you did. Thank you."

The Lietzau Era
"By the Numbers"



VISION FOR AMERICA'S GATEKEEPER

By Wally Coggins
Chief Strategy Officer

DCSA'S VISION FOR AMERICA'S GATEKEEPER

In 2019, when several security organizations formed into the Defense Counterintelligence and Security Agency (DCSA), DCSA's vision looked to optimize performance through the transfer of its core missions into one unified agency. In the years since, DCSA began implementing its first Strategic Plan (2022-2027), through which the agency achieved record improvements to mission performance in support of national security across all mission elements. Within the same time, the strategic challenge of Great Power Competition and pervasive insider threats has produced new kinds of threats to the Nation's defense industrial base and broader trusted workforce. DCSA's role in national security is expanding, requiring the agency to refine its initial vision as America's Gatekeeper. In June 2023, DCSA published - a new vision, which looks toward a future of integrated mission functions that will enable DCSA to become the premier provider of integrated security services to counter the growing threats confronting the Nation.

DEFENDING THE GATE THROUGH UNITY OF EFFORT

DCSA's vision focuses on driving unity of effort internally and externally to advance priorities across three areas of focus. First, DCSA optimizes its core personnel and industrial base vetting missions through increased integration and information sharing. Second, DCSA leads the security community with training, threat awareness, and information sharing protocols. Third, DCSA is the employer of choice with state-of-the-art workplace capabilities. Success across these three areas will require enhanced collaboration within DCSA, and between the agency and the broader security enterprise, to include our government and industry partners.

FORGING ONE GATEKEEPER CULTURE

The final words of the vision statement clearly state, "national security is our mission, people are our greatest asset." DCSA draws the most committed and talented security professionals in the country. Our people are our greatest asset, and DCSA is proud of the Gatekeeper culture that its outstanding workforce fosters. As DCSA looks ahead, the challenge of seizing the opportunities for greater national security outcomes hinge on the dedication of its people. In this respect, the Gatekeepers of DCSA prove to be the agency's most critical advantage. DCSA's values of mission, people, service, integrity, and innovation is a major draw for the workforce, who live these values. This is fundamental to the mission, and essential to the success of the agency. DCSA remains focused on people and will continue to be intentional in everything it does as an organization to build the DCSA Gatekeeper culture.

ASK THE LEADERSHIP

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

James Shappell, serves as the Deputy Assistant Director (DAD) for Defense Insider Threat within the Counterintelligence and Insider Threat Directorate, also filling the role as the Director of the DOD Insider Threat Management and Analysis Center (DITMAC)

In this position, he serves as the senior advisor to the DCSA Director on insider threat and oversees all DOD-level operations, program management, and business/support of the DITMAC..

Prior to joining DCSA, Mr. Shappell served as the Chief of Staff at the National Intelligence Council at the Office of the Director of National Intelligence (ODNI). He also served in multiple positions at the U.S. Army Intelligence and Security Command (INSCOM), including the Acting Assistant Chief of Staff (ACoS), G-2; creating, establishing, and leading the INSCOM Security Operations Center as its first director; the Deputy ACoS, G-2; and the Command Security Manager and Special Security Officer. He also served as a security specialist at U.S. Army Yuma Proving Ground.

Prior to his civilian career, Mr. Shappell served four years on active duty as an intelligence analyst, primarily supporting operations in the Republic of Korea.

Throughout his career Mr. Shappell earned a number of awards including the Army Commendation Medal and two Army Achievement medals for his service on active duty. He received the ODNI Exceptional Service Award, the Army Commander's Award for Civilian Service, and two Army Achievement Medals for Civilian Service.

In addition to his professional experience, Mr. Shappell has a dual Master of Arts degree in Leadership and Management and Security Management and Administration from Webster University, a Bachelor of Science Degree in Communications from Mansfield University, and an Associates of Applied Science in Intelligence Operations from Cochise College. He completed the Wharton School's Certificate in Leadership and Management and the Federal Executive Institute's Leadership for Democratic Society, and received the Carnegie Mellon's Software Engineering Institute's Insider Threat Program Manager Certificate. He has achieved the DOD Certified Counter-Insider Threat Professional – Fundamental.

QUESTIONS AND ANSWERS

We have your bio, but what would you like reader to know about you? What brought you to this job

I love serving my country and leading change, so coming to DCSA was an opportunity to do both. I was at the Army's Intelligence and Security Command when DITMAC was established, and had a chance to work with the folks who helped stand it up. I came here originally to be the chief of analysis and mitigation and then was promoted up. Now things are changing rapidly and it's a really exciting time to be a Gatekeeper.

What do you want to make sure people know and understand about DITMAC?

First, the people who work at the DITMAC are amazing and passionate – it's a great team, and that team executes seven different mission areas to support the DOD insider threat enterprise in identifying and assessing risk. With that said, we can't be viewed as the all-knowing "silver bullet" to stop any insider action. A big part of our efforts is focusing on information we get from the 43 component insider threat hubs, and working with them to assess risk and mitigate it. It's a collaborative effort that continues to improve and be refined, and we bring a lot of really good tools and expertise to that effort.

We know DITMAC was established in the wake of the Washington Navy Yard shooting. How has the awareness and understanding of the insider threat changed since this incident?

It's a really good question, and I think some of the challenges we face in the Department of Defense stem from the sheer size of the organization, the information stovepipes we continue to try to break down, and the stigma of the word "threat" early in the process. Helping people understand that the risk indicators we see are potentially indicative of someone becoming an insider threat is important, helping them understand not everyone becomes an insider threat who portrays those risk indicators, and there are ways to help people get off the critical pathway to violence or espionage, are keys. I think the insider threat community has done a good job of communicating with each other, and we see pockets of excellence in how programs are able to do this across DOD, however, it has not taken hold holistically, and we still have a lot of work to do to help people understand how the program can actually be a value to commands and agencies.

What are the biggest challenges facing DITMAC right now?

I think we've had a really great opportunity to expand our mission capabilities over the past 12 months as we implement newly required missions and more than double our workforce. So the challenge over the next 12 months is looking at how we continue to improve those, along with our existing capabilities, and integrate them into the broader insider threat ecosystem. Those missions and resources are really a down payment the Department made on improving our ability to respond to emerging risks, and we'll need to be able to show return on that investment in the future. So, we need to ensure all our new team members can see themselves in the Gatekeeper culture and understand how important the work they are doing is to the rest of the Department. None of that is easy, but it's such a unique opportunity to be at the tip of the spear on a new initiative, and that also makes it really exciting.

Can you expand on the less known DITMAC missions?

Sure. I think a lot of people are probably familiar with the DITMAC's analysis and mitigation mission, which is the part that works with components to identify potential threats and help to mitigate them. But like I said earlier, there are really seven distinct missions within the DITMAC.

The Unauthorized Disclosure Program Management Office (PMO) serves a unique role in coordinating with DOD elements that have classified or controlled unclassified information appear in the public domain. This means working with them to help reduce the potential suspect pool of personnel who may have committed the leak and evaluating the damage to national security, then coordinating with the Department of Justice if there's an investigation to follow. If there's a reported UD, they are also authorized to go view the data and pull it off the open web to allow components to look at it side-by-side with source documents.

I think another big one, one of those new missions I mentioned, is our Assessment and Professionalization division. So far we've done assessments of five DOD insider threat programs this year. We are going beyond what the national minimum standards are, and looking at the maturity framework model to determine whether programs are effective and efficient. So this isn't just a "check the block" to ensure documentation is on hand, it's really looking at how programs are implementing what they have documented as their policies and procedures, and determining the overall ability of a program to actually assess risk from trusted insiders. We've received really great feedback from components that have gone through the assessments, and I think this is going to be a critical tool in the DITMAC portfolio moving forward to help the broader insider threat community.

There seems to be a lot of misconceptions concerning UAM, like big brother is watching you. What does UAM actually do?

At a high level, UAM is basically the ability to identify anomalous behavior of users on the network. Depending on the quality of the tool used, the policies or triggers that are established, and the bandwidth of analysts on an account, it can help to see things as simple as violations of cybersecurity policies, or specific references to documents, classified markings on the unclassified system, or even potential threats.

I guess in regards to the "big brother" comment, what I'd offer is insider threat programs don't have the time or the mission to log, research, and look at everything people are doing. What's covered under UAM will typically go through General Counsel and privacy channels for a review and the triggers have to be well researched and developed. In fact, part of the requirements for insider threat programs is to have training on privacy and civil liberties. It comes back to the idea of us wanting to create an environment where the workforce can trust us, and part of that is ensuring that we uphold the strictest standards in evaluating how we run programs like UAM.

Prevention, Assistance and Response (PAR) was initially introduced as a concept following the Fort Hood Shooting. Based on the DITMAC's mission to close gaps and lead the DOD insider threat enterprise, managing centralized capabilities to provide this support at the 12 joint bases and regions across DOD is a logical next step. Where are we in the implementation of PAR? And what are the future PAR plans?

We are making good progress on getting PAR off the ground, and I give a lot of credit to our PAR Chief, Dave Paravecchia, who has been leaning forward and coordinating with the Office of the Under Secretary of Defense for Personnel and Readiness and the prevention workforce to get the program coordinated, while also working with those 12 bases and getting hiring efforts completed. Right now, we have at least one person at every joint base location and they're doing the very hard work of building networks, getting a seat at the table, and gaining the trust of their partners at those locations. Because the program has never been fully implemented, and this is one of the new missions that fall into the category of seven, it's a real challenge. But we are finding that commanders are starting to embrace the idea of having someone available to them that can help them assess the risk. And that's really what I view PAR as being – a tool to help commander's make informed, risk-based decisions. The decisions on action still largely remain with those people closest

to the issue, and so using a network of personnel knowledgeable in threat assessment and management is a great opportunity to improve their ability to understand the risk he or she may be accepting.

We hosted the first PAR training in August at the Russell-Knox Building in Quantico, with all our onboarded PAR coordinators attending. We had participation from our Behavioral Threat Analysis Center, or BTAC, which is our in-house network of subject matter experts in behavioral health, threat assessment and management, counterintelligence and law enforcement, cybersecurity, and management-employee relations. The BTAC, another of those seven missions, will be a reach-back capability for PAR coordinators, help to train and professionalize them, and will also support analytic work done by our analysis and mitigation. It's a really integral part of our efforts across the board to identify and assess risk and inform appropriate stakeholders of potential options for mitigation.

And of course, this all has to be coordinated with those 43 components, because we are talking about individuals that fall within their purview. It's a good example of how we, DITMAC, play an integral part of the insider threat ecosystem.

What's next for DITMAC?

I wish I had the magic 8 ball to predict this one. We have some additional PAR coordinators to bring onboard this fiscal year, and we have a lot of work to do to integrate all these new missions into the existing DITMAC and DCSA infrastructure. We've done some good cross-training with adjudicators at the Consolidated Adjudication Services, or CAS, and I'd like to see us continue to work with the Operations Analysis Group and Industrial Security to explore how the agency can further provide insider threat support to industry. And we are working closely with the Program Executive Office to help evolve the systems-based capabilities for the insider threat enterprise.

So for now we have a pretty heavy lift, but we know there's a lot of opportunities for us to support Trusted Workforce 2.0, Zero Trust, and Integrated Prevention Program initiatives within the Department, and we are happy to keep partnering with our colleagues to find the right ways to integrate our mission with theirs. I know this much, we won't be bored!

Agency supports NITAM events, increase insider threat awareness, mitigation resources

In support of National Insider Threat Awareness Month, the Defense Counterintelligence and Security Agency either hosted or participated in several events and activities. The following list is a sampling of those events.

NITAM
National Insider Threat Awareness

On Sept. 6, the DOD Insider Threat Management and Analysis Center (DITMAC) supported the Pentagon Insider Threat Awareness Day.

On Sept. 7, DCSA sponsored the Virtual Insider Threat Conference. Keynote speaker was Andrew J. Lochli, assistant director, Counterintelligence and Insider Threat Directorate. The conference also covered such topics as counter-insider threat professionalization, organizational resources, toolkits for insider threat mitigation, etc. When available, you'll find a recording of the conference here: https://www.cdse.edu/Training/Webinars-and-Conferences/Conference-Archive/

On Sept. 14, the Center for Development of Security Excellence and the U.S. Navy jointly hosted the webinar, "The Washington Navy Yard Shooting: 10 Years Later and a Survivor's Account," which focused on the immediate and long-lasting impacts of the WNY shooting. You can find the archived recording here: https://www.cdse.edu/Training/Webinars-and-Conferences/Webinar-Archive/The-Washington-Navy-Yard-Shooting-10-Years-Later-and-A-Survivors-Account/

On Sept. 19, CDSE offered the "Espionage in the Era of Insider Threat" webinar. When available, you'll find a recording of the webinar here: https://www.cdse.edu/Training/Webinars-and-Conferences/Webinar-Archive/

CDSE supported the Department of Justice Insider Threat Symposium on **Sept. 23**.

At the DSI Insider Threat Symposium, **Sept. 27-28**, James Shappell, director of DITMAC, was the first speaker at this two-day event.

Launched the updated NITAM website, https://securityawareness.usalearning.gov/cdse/nitam/

New DOD Prevention, Assistance and Response cadre assist commanders in assessing insider threat, workplace violence risk

By John Joyce
Office of Communications and Congressional Affairs

Brittani Blanchard trained with the Prevention, Assistance and Response (PAR) cadre assigned to military installations across the country – including Hawaii, Alaska and Guam – for the first time and envisioned the PAR program's future impact upon U.S. military and national security.

The Defense Counterintelligence and Security Agency (DCSA) PAR office chief for the National Capital Region collaborated with her counterparts throughout intensive training sessions at the PAR Cadre Training Seminar held at DCSA's Quantico headquarters from Aug. 7-10.

Now, Blanchard – a four-year DCSA employee who is "very passionate about behavioral health education, training and awareness" – looks forward to a future of PAR coordination with her colleagues as they leverage new and emerging capabilities to provide military commanders and their civilian equivalent leaders with an understanding of overall risks within their organizations as well as options to care for their personnel that could result in a significantly reduced risk of insider threat and workplace violence.

"This is an opportunity to meet our teammates as we practice and see what it takes to be successful in the position as a PAR office chief or as a PAR coordinator," said Blanchard, who also serves as PAR office chief for the DCSA Mid-Atlantic Region. "It's crucial for our entire team to be level set and on the same page regarding what the Prevention, Assistance and Response program is, the tools and assessments we are using, and how we should execute the program across DOD at our respective installations. This unification entails an effective communication strategy to convey to our various communities – military members, civilians, and their families – what we're doing. As PAR coordinators, we have diverse backgrounds and expertise, but we have knowledge, expertise and resources in common that are essential in order to effectively execute this hard mission."

National Capital Region PAR Office Chief Brittani Blanchard is pictured during an interview at the Prevention, Assistance and Response (PAR) Cadre Training Seminar held at DCSA's Quantico headquarters from Aug. 7-10. (DOD photo by Christopher P. Gillis)

The intense training for the PAR program – a newly formed capability under the direction of the DOD Insider Threat Management and Analysis Center (DITMAC) – prepared the new PAR coordinators to fulfill their roles supporting commanders and equivalent civilian leaders on installations and in the military community by conducting threat assessment and management, primarily focused in the area of workplace violence.

"PAR is more than counterintelligence and security. You've got to be able to talk with the experts who are looking at suicide prevention and sexual assault prevention and response – all of those different aspects – and understand what recommendations can be made to help people

get into those capabilities that can help them," DITMAC Director James Shappell advised the PAR audience. "That's a tough but an exciting job because you can actually see differences that you'll make on the ground. So, talk to those folks and understand their programs and what you can pull from their programs to incorporate into your PAR efforts and talk to folks at the local levels about how you integrate with them."

Although recently hired, addressing risk – deterring, detecting, assessing and mitigating violent behaviors and actions – is not new to the PAR professionals with former careers predominantly in the counterintelligence, law enforcement and security communities spanning leadership positions from the private sector and state law enforcement to DOD and the federal government.

Dave Paravecchia, chief of the DOD Prevention, Assistance and Response (PAR) Division at the DOD Insider Threat Management and Analysis Center, briefs PAR coordinators at the PAR Cadre Training Seminar held at DCSA headquarters in Quantico, Va., on Aug. 7. (DOD photo by Christopher P. Gillis)

"However, the transition many will make in this position is to understand their greater role in the prevention and assistance portion of their mission versus just responding to danger," said Dave Paravecchia, chief of the DOD PAR Division at DITMAC, in an interview during the seminar. "Specific to workplace violence, the PAR cadre are trained on indicators of violent behaviors, friction points in an individual's life which may be influencing their behaviors and actions, data aggregation, threat and risk assessment, subject professional judgement tools, coping mechanisms, available services and other mitigation measures that can be implemented by military and civilian leaders to help move someone off the path of violence."

In all, 36 PAR coordinators will utilize a multidisciplinary approach through collaboration with trained professionals, integrated prevention experts, and key stakeholders to develop tailored risk assessments and mitigation strategies while leading PAR programs at 12 joint bases or regions and five service specific military installations in fiscal year 2023.

DOD Prevention Plan of Action 2.0

"You are the component PAR team on the ground doing the goodness of what this program is here to do – help the military services get after workplace violence issues," Paravecchia told the PAR coordinators on the seminar's first day while briefing the cadre on their role in implementing DOD's Prevention Plan of Action (PPoA) 2.0. "We are asking you to ensure that commanders are situationally aware of the risks on their installation."

The PPoA 2.0 approach focuses on integrated prevention that will require finding shared solutions to the problems of workplace violence, sexual assault, harassment, retaliation, domestic abuse, suicide and child abuse. This range of harmful behaviors – which share many risk and protective factors – require diverse and unique prevention approaches.

"We follow this PPoA to achieve our ultimate goal – reduce workplace violence," Paravecchia told the PAR cadre while describing how it will align competing priorities, increase program effectiveness, ensure efficient use of resources, and help leaders cultivate safe and healthy climates across the military community. "This strategy guides how we do prevention in the DOD. The other prevention subject matter experts use it to reduce sexual assault, child abuse and domestic violence. You're going to work side by side with other stakeholders in the violence arena."

In their efforts to prevent workplace and other violent issues, PAR cadre will present briefings to the military community and conduct outreach, education and training on reporting and indicators of violence to help individuals understand when problems may be arising.

PAR Coordination, Collaboration and Advisement

As they provide assistance, PAR coordinators will work closely with prevention and human resource experts to ensure military and civilian leaders are aware of various services such as financial planning, marriage counseling and other employee assistance programs while assisting them in dealing with any friction points in their lives that are causing them to act or behave violently.

In terms of response – if the PAR professionals learn that an individual is beginning to escalate further down the path of violence – they will work closely with law enforcement, security and leadership to better understand

DCSA Director William Lietzau briefs PAR coordinators at the PAR Cadre Training Seminar held at DCSA headquarters in Quantico, Va., on Aug. 7. (DOD photos by Christopher P. Gillis)

the risk and help develop potential mitigation measures to stop the threat.

"We're trying to prevent the next Fort Hood," DCSA Director William Lietzau told the PAR audience in his welcoming remarks at the seminar. "I'm giving you free rein to think outside the box. You don't have the benefit of having someone to do a turnover with. There's no SOP on the desk when you get there. There's no right answer. You have to come up with it. You are creating policies."

Since the Fort Hood – now known as Fort Cavazos – Texas, shooting in 2009, DOD continued to suffer from high profile violent and active shooter events at military installations, including the Washington D.C. Navy Yard in 2013; Fort Hood in 2014; Fort Leavenworth, Kan., in 2016; Naval Air Station Pensacola, Fla., Pearl Harbor-Hickam, Hawaii, in 2019; and Fort Stewart, Ga., in 2022.

"I need you to figure out how to solve problems. This is a people-oriented business and it's true of all of our programs at DCSA but in your case especially," said Lietzau, regarding the necessity for the PAR cadre to address issues and behaviors as early as possible by recognizing a risk an individual poses, making services to help the individual available, and working to remove individuals from the path of violence to salvage careers and maintain unit readiness and cohesion.

"The biggest thing you can do from my perspective is to get to the place where for whatever reason – religious, personal comprehension of leadership styles, any reason – is to empty yourself of personal motivations that may cause you to do something for your own career advancement and work on behalf of the organization, the mission and the people that you lead," Lietzau advised. "You're going to be in a situation where you may very well prevent something and I'm going to thank you now for preventing the tragedy that no one can give you credit for. It's the nature of your job – being selfless to do things that you know is good for the country. It's not grand and while you're doing it – figure out how we can better set up this system so that we can do it in a broader way across the federal government to save lives and accomplish our mission."

PAR Mitigation and Prevention Pressure Points

The commanders at military installations – from Army garrisons to Navy, Marine Corps, Air Force and joint bases – can anticipate motivated, collaborative and innovative PAR professionals from DCSA who will pay close attention to workplace violence issues within the installations' organizations and communities.

"DCSA is so well placed in industry, academia and across the hubs to really contribute and make an impact –

Andrew Lochli, assistant director for Counterintelligence and Insider Threat, briefs PAR coordinators at the PAR Cadre Training Seminar held at DCSA headquarters in Quantico, Va., on Aug. 7.

leverage this agency," Andrew Lochli, DCSA assistant director for Counterintelligence and Insider Threat, advised the PAR professionals. "If someone is not suitable to hold a clearance, that's the mitigation we need. If someone needs to go to family advocacy to get some help and that takes them off the critical path, that's the mitigation we need."

The mitigation is accomplished as PAR coordinators advise the commander and base leadership in the prevention, assistance and response to potential threats while they gather information and work with stakeholders and members of the commander's staff. The information includes a holistic assessment of an individual or threat in

order to make recommendations that will raise awareness, assist with leader decision making, and help prevent and reduce risk.

"I think back to my time as an analyst in the DITMAC Analysis and Mitigation Division as we're getting the PAR program set up to help stop people from making career ending decisions, to prevent them from hurting their fellow community members, to maintain unit readiness and enhance unit cohesion," said Blanchard. "I proactively look for those prevention pressure points, like where can we be the most effective in preventing an issue, stressor or incident from escalating or turning into a loss of life. It's always important to take a step back and consider a whole person concept and being empathetic, asking, 'what is this person possibly going through' in order to provide our most effective PAR response."

The remedy to prevent a potential act of workplace violence and put that person on the right track may be as simple as financial or marriage counseling.

"Catching indicators at its earliest stage can really help deter people from committing acts of violence against their workplace," said Blanchard. "It also enhances the morale of personnel. People are able to recognize and appreciate that their leadership cares enough to notice that there is something wrong and take action to help them."

In the case of someone who progresses too far down a path of violence, when it's too late to render prevention and assistance, the response tenet requires PAR coordinators to ensure law enforcement, security and insider threat personnel are aware of the situation if they are not already involved.

All aspects of the PAR program development from education and training to collaboration and policy making will continue in the wake of the training seminar's conclusion. A yearlong assessment of the program will move through three phases of its initial operating capability until DCSA DITMAC judges the program fully operational. This decision is scheduled for the first quarter of fiscal year 2025.

"We will continue to mature the PAR program in collaboration with our stakeholders in prevention, law enforcement, security and insider threat to decrease the prevalence of violence on different installations, military services and the department," said Paravecchia. "Over time, we will shape various metrics that will help highlight the return of investment in this program and improve awareness for leaders where workplace violence issues may exist within different subordinate commands and organizations."

PAR Program History

The PAR program was originally developed as a result of the Fort Hood mass shooting in 2009.

In 2017, DOD issued a memorandum entitled 'Final Implementation Actions of Fort Hood Recommendations: Managing Risk of Potentially Violent Behavior through Prevention, Assistance, and Response Capabilities,' outlining PAR requirements throughout the department.

In June 2022 – to further PAR capabilities across DOD – DCSA was given the mission to establish a centralized PAR capability that standardizes implementation of insider threat program requirements while reducing DOD component concerns about organizational responsibilities and resourcing requirements.

The DCSA PAR program – one of several programs being implemented in response to the June 2022 order to expand and modernize DOD's enterprise insider threat efforts – also includes:

• A centralized Behavioral Threat Analysis Center.

• A robust DITMAC System of Systems information technology capability to enhance case-management capabilities and advanced analytics to identify trends.

• An Insider Threat Assessment program.

• A DOD Workforce Insider Threat hotline to create a department-wide virtual, anonymous reporting capability, and triage management center.

A Dec. 12, 2014, memorandum issued by the Office of the Under Secretary of Defense (OUSD) for Intelligence – now OUSD for Intelligence and Security – directed the establishment of DITMAC and its concept of operations. As a result of insider threat program evolution, the memorandum includes the current PAR program among other programs that are intended to support insider threat activities in the military services, the intelligence community, and DOD agencies through the development, implementation and sustainment of technologies that aid in the management, analysis and mitigation of insider threat information.

DITMAC maintains cadre of SMEs to assist in the analysis of insider threat information

By Allison Wolff
DOD Insider Threat Management and Analysis Center

Every person working for the federal government is an insider, and everyday each person brings with them a different set of insider threat risks. Many trusted insiders are people we rely upon to safeguard the nation's critical systems, data, intelligence, and military plans. From malicious actors to negligent employees, insider threats come in many forms and can have devastating consequences. Prevention and early identification of insider threat indicators are essential to deter and interrupt existing concerns. The DOD Insider Threat Management and Analysis Center (DITMAC) is charged with consolidating and analyzing insider threat-related information to facilitate early detection of potential insider threats. The DITMAC makes recommendations influencing decisions to decrease the impact and risks associated with insider threats on the workplace.

Established following the 2013 Washington Navy Yard mass shooting, the DITMAC develops a holistic picture of insider risk and accordingly coordinates mitigation responses. This consolidated enterprise-wide analytic capability closes critical information gaps by connecting components, individuals, information and data points. DITMAC provides a centralized repository for insider threat information and coordinates with programs across the Department of Defense (DoD) to ensure that all affected parties have the information they need in order to deter, detect and mitigate insider risk.

Behind the scenes, DITMAC maintains a cadre of subject matter experts (SMEs) in a variety of disciplines to assist in the analysis of insider threat information. Individuals with expertise in the areas of behavioral psychology, threat

James Shappell, DOD Insider Threat Management and Analysis Center (DITMAC) director, briefs Prevention, Assistance, and Response (PAR) coordinators at the PAR Cadre Training Seminar held at DCSA headquarters in Quantico, Va., on Aug. 7.

analysis and management, counterintelligence and law enforcement who serve as consultants to DITMAC analysts and also directly engage with insider threat and security professionals across the DOD to assist with the analysis of potential threats and thereby closing knowledge gaps.

"The DITMAC plays a critical role in helping the DOD's insider threat community to assess risk early in the process," said James Shappell, Defense Counterintelligence Security Agency's (DCSA) Deputy Assistant Director for Defense Insider Threat who serves as the Director of the DITMAC. "The hope is that this early intervention stops people from actually becoming insider threats who pose an increased risk to other personnel, information, facilities, and assets." These risks can also include things like workplace violence, domestic violence, suicide and espionage.

Today, the need for DITMAC's functional expertise is growing and the mission is expanding in both roles and responsibilities. DCSA is approaching these new roles and responsibilities as "DITMAC Modernization," and it represents an opportunity for the continued growth of a robust insider threat capability across the Department.

"The effort to modernize the capability and approach of the DITMAC really allows us to provide more robust support to the defense insider threat ecosystem," said Shappell. "The combination of new capabilities and existing capabilities really starts to put us in a better place to see things as they are happening, and hopefully affect positive

change before an event happens."

Prevention, Assistance, and Response (PAR)

One of the key tenets to the successful management of risk is identifying threats at their earliest instance. The Prevention, Assistance, and Response (PAR) program is one of the capabilities that DITMAC will oversee to focus on early identification of potential insider threats.

Find out more about the PAR program and the training for the initial cadre of PAR coordinators by reading the cover story, which starts on page XX.

Behavioral Threat Analysis Center

The newly established Behavioral Threat Analysis Center (BTAC) will grow expertise by increasing the number of SMEs in existing fields (including behavioral psychology, counterintelligence and law enforcement, and threat assessment and management) and expanding to add experts in cybersecurity and management employee relations.

BTAC SMEs evaluate challenging and complex cases of insider risk, and collaborate in formulating mitigation strategies that are specifically tailored to each unique case. SMEs also develop training on topics within their area of expertise and identify areas of research that will enhance knowledge and assist PAR cadre and insider threat professionals to improve their knowledge, skills, and abilities.

The integration of PAR cadre at the DOD installation level coupled with the insights of the BTAC SMEs will provide a more holistic approach to insider risk mitigation and knowledge sharing. These expanded capabilities serve to inform leaders with more timely and comprehensive recommendations and allow for more informed risk-based decisions.

Enterprise Program Management Office

The PAR program and BTAC SMEs are part of DITMAC operations and work alongside an expanded Enterprise Program Management Office (EPMO) which oversees a wide range of capabilities. EPMO originally had a smaller scope, but is growing to support functional areas including:

- Unauthorized Disclosure (UD) Program Management Office - coordinates reporting of UDs and facilitates the delivery of crime reports and referrals to DOJ
- Performance, Requirements, Information, Standards and Metrics Office (PRISM) - fosters innovation and collaboration across the DoD Insider Threat (InT) enterprise through development of advanced metrics
- Publicly Available Information (PAI) capability- integrates new sources of PAI into InT analytic products to contextualize risk.
- Assessment and Professionalization- described below

The EPMO capabilities are expanding to more fully support the growing need, depth and breadth of insider threat requirements. These functional support areas directly align to the customer's needs and further enhance the DITMAC's expertise in insider threat risk and mitigation strategies.

Assessment and Professionalization Program

Within the EPMO, DITMAC is developing a team specialized in Insider Threat Program Assessments and Professionalization. DITMAC's Assessment team facilitates and reviews DOD component insider threat programs to advance their capabilities and not only achieve the national minimum standards as outlined by the National Insider Threat Task Force but to take those programs to standards where they are truly efficient and effective. DITMAC coordinates between 43 Insider Threat hubs to assist them from program establishment through initial operating capability until they achieved full operating capability, and then helps them to navigate the maturity framework model to improve the overall program capabilities. This team provides a structured framework evaluation of programs to determine the overall level of effectiveness and provides recommendations to enhance it.

The professionalization program is working closely with a number of entities across the DoD to standardize a pathway to certification and professionalization of insider threat personnel. These two elements together will enhance DOD's ability to identify and assess risk from trusted insiders early and in a standardized manner.

From expertise to training, the recent DITMAC Modernization effort is holistically expanding in mission and capacity. These new capabilities tie directly into what customers are doing at their level to mitigate risk early in the process, be more resilient, and support the national security mission by sustaining a trusted workforce. Together, the DITMAC is serving the Department of Defense to mitigate potential insider threats.

OCIO successfully completes concurrent enterprise cybersecurity audits

By Adam Miller
Office of the Chief Information Officer

The Defense Counterintelligence and Security Agency (DCSA) recently underwent two simultaneous cybersecurity audits conducted by the Joint Forces Headquarters – Department of Defense Information Network (JFHQ-DODIN): a Command Cyber Readiness Inspection (CCRI) and an annual inspection of the Public Key Infrastructure (PKI) Program. The results indicate that DCSA is poised to be a leader in the DOD based on the achievement rating of the PKI assessment and as the first agency to achieve a Low Risk designation across all DOD for the CCRI 3.0 Pilot inspection.

The JFHQ-DODIN is the enforcement arm for regulatory policies established by the DOD PKI Program Management Office. Together, these entities govern PKI operations and support activities throughout the DOD Enterprise.

Both inspection efforts were led by DCSA Chief Information Security Officer (CISO) Roxanne Landreaux, under the Office of the Chief Information Officer Jeanette M. Duncan.

Public Key Infrastructure (PKI) Program Inspection:

The DCSA Enterprise Public Key Infrastructure (PKI) Program, within the OCIO/CISO, achieved a 98% rating during its 2023 annual inspection conducted by JFHQ-DODIN. This achievement marks the second time in less than 12 months, and the third time since 2020, that the PKI Program has scored in the top 5% across DOD components.

The DCSA PKI Program is a critical support function for the enablement of secure enterprise information technology (IT) services. The PKI program manages the lifecycle of tokens required for accessing classified networks, and administrative access to both classified and unclassified computing environments. In addition, Public Key Encryption-based certificates approved through the program enables confidentiality, integrity and availability protection for DCSA infrastructure and application platforms. Hence, the scope of PKI within DCSA spans the core (infrastructure), distribution (networks), and access (end-points) layers of the enterprise from DCSA headquarters in the Russell-Knox Building to 40-plus remote sites across the United States.

The extent of human, device, and software entities throughout DCSA requiring PKI-based credentials is enormous and cyclical. Certificates (or tokens) associated with each entity have a limited lifespan of 36 months and must be reissued prior to expiration or shortly thereafter. Program success hinges upon concerted efforts among technical, customer support, information security, and management staff.

Such efforts were the focal point of the 2023 PKI Audit, which entailed individual interviews across a number of trusted roles. The audit's scope encompassed programmatic, business, information security, and IT processes. The inspection covered 112 audit items including subtasks, all of which were measured against national security systems standards.

The success of this audit is attributed to the following individuals within the OCIO:

PKI Audit Leadership: CISO Roxanne Landreaux, Cybersecurity, Compliance and Risk Management Division Chief

Site Points of Contact: Gidel Mendez, Cyber Compliance and PKI Branch Chief

PKI Program Manager: Michael Cruz

Self-assessment Coordinators: Brian Brown and Christian Johnson

Registration Authorities: James Wright and Dale Rolfe

Information System Security Officers: Jonathan Evans and Phillip Mathews.

Command Cyber Readiness Inspection (CCRI) 3.0 Pilot:

The Command Cyber Readiness Inspection (CCRI) program is a thorough audit of an agency's cyber posture and determines the risk and security of its data and systems. CCRI inspections, conducted by certified DOD teams under the direction and authority of U.S. Cyber Command and JFHQ-DODIN, determines an agency's cyber authority critical to the protection of DOD networks.

Due to the CCRI 3.0 effort being in its Pilot phase, it consisted of fluid scoring parameters and a much more stringent risk threshold from previous scoring structures. Many eyes from around DOD were fixated on DCSA as it was only the second agency to be assessed under JFHQ-DODIN's new and untested pilot program. Multiple DOD stakeholders were concerned that achieving a passing score would be all but impossible under the 3.0 assessment rubric, and that anything but a Low Risk score would increase the likelihood of information systems being disconnected from the network.

Through partnership with the JFHQ-DODIN audit team, thousands of hours of hard work from OCIO's cybersecurity professionals, and strong leadership from the DCSA Audit Assessment Team led by CISO Roxanne Landreaux, DCSA was the first agency in the DOD to achieve a Low Risk posture according to JFHQ-DODIN's 3.0 pilot scoring methodology.

The collaboration between JFHQ-DODIN and DCSA was so thorough that JFHQ-DODIN has updated its methodologies for future audits by adopting DCSA's vulnerability risk assessment, tracking, and closure methodologies as gold standard CCRI 3.0 practices to be emulated by all DOD components.

The following are attributed to the success of the CCRI 3.0 audit:

CCRI Audit Coordinators for DCSA: Farley Jones (Cybersecurity, Compliance and Risk Management Division / CRAM Chief) and Christopher Haskell (CCRM/ CRAM CTR)

DCSA Audit Leadership: CIO Jeanette M. Duncan; CISO Roxanne Landreaux

DCSA Audit Team Leads: Si Troung (Enterprise Operations); Gidel Mendez (CCRM/ CCP); Dave Hobbs (Enterprise Operations); Bruce Fredette (CCRM/ CWC Chief); Eric Corbin (Customer Support Chief); Jessica Kemp (CCRM/ CDO); Ruben Rios (CCRM/ CAMO Chief); Jonathan Evans (CCRM/ CRAM); James "Jim" Hughes (CCRM/ CDO Chief)

Conducting assessment/audits of the agency's operating environments are critical to ensuring the protection of the mission of the DCSA, as well as follow all pertinent regulations directed by the DOD. The agency's final scores are a testament to the teamwork and professionalism of all involved in both the PKI and CCRI audits. The Cyber Compliance and Risk Management Division, led by Landreaux, continues to demonstrate cybersecurity excellence through self-assessments that continue to improve the agency's effectiveness and efficiencies when facing new and emerging threats.

DCSA employees receive NCMS industrial security awards

During this year's annual NCMS training seminar, held June 5-8, in New Orleans, La., three DCSA employees received NCMS Industrial Security Awards for 2023.

Receiving Industrial Security Awards were:

- Jennifer Norden, Regional Mission Director for Industrial Security, Central Region, Field Operations
- Robert Gerardi, Field Office Chief, Melbourne (Fla.) Field Office, Field Operations
- Sal Urbano, Industrial Security Representative, St. Louis Field Office, Field Operations

NCMS President Lynn Burns (left) presents NCMS industrial security awards to DCSA employees (from left) Robert Gerardi, Sal Urbano and Jennifer Norden. (Photo courtesy of NCMS)

Jennifer Norden

According to the award nomination, Norden made monumental contributions to the protection of classified information. She was the DCSA Irving (Texas) Field Office Chief, responsible for administering the National Industrial Security Program for approximately 400 contractor facilities in North Texas, Oklahoma, Kansas, and Arkansas. She served as the region's subject matter expert on industrial security policies, including foreign ownership, control or influence. Norden has been a key figure within the Dallas-Fort Worth (DFW) area through her collaborations with the Greater DFW Chapter of NCMS and the Joint Security Awareness Council (JSAC) planning committee. She was the key speaker for the DCSA field office and the ringleader that brought regional leadership to each JSAC conference. She made it a priority to connect with industry by maintaining constant communications via email or teleconference while the legacy Defense Security Service was undergoing DSS In Transition and during the implementation of 32 Code of Federal Regulation, Part 117, "National Industrial Security Program Operating Manual," Rule. Norden has strongly partnered with NCMS, encouraging participation, and working with the local chapter chairs and board of director members to present at meetings and ensure awareness of changes in industry.

"We in DCSA are the designated Gatekeepers for our nation, but we cannot be successful in that role without effective communication and relationships with our Industry stakeholders," she said. "The more we understand our mutual security interests and work together to address our mutual challenges, the stronger our national security posture. In my experience, NCMS has been a key factor in this communication and relationship equation by providing forums across the country to discuss these interests and challenges.

"This award is 'Boots on the Ground' recognition from a community that knows firsthand the dedication needed by all parties to continuously and persistently invest in relationships for the greater good of national security," Norden said, noting that is why it is "one of the most appreciated recognitions in my DCSA career."

Robert Gerardi

According to the nomination package, Gerardi became the chairperson of the Florida Industrial Security Working Group (FISWG) in 2020, while working in industry, and continues as chairperson under DCSA until a successor can be found. He ensured that quality training was provided across many security disciplines throughout the region, free of charge.

During COVID-19, when meeting in person was no longer an option, Gerardi teamed with the NCMS Florida Sun Coast chapter and the combined group shifted to a virtual environment to ensure the security community continued to receive relevant training in a timely manner. His quarterly training events equated to 13,000 man-hours of training in a wide array of security disciplines and by leveraging the NCMS Web-X platform and the FISWG membership base, Gerardi more than tripled the attendance. These events benefited the industrial security base across the board. The virtual training events were widely advertised, and non-members soon learned the opportunities offered by NCMS, increasing membership in both the Sun Coast chapter and FISWG. The continued efforts to put on these training events serve as a force-multiplier, strengthening overall security compliance to the National Industrial Security Program and furthering the protection of classified material entrusted to industry.

"This award signifies that we are doing 'the right thing' by providing these training events," said Gerardi, who became the Melbourne Field Office Chief in July. "During the NCMS conference, I had many facility security officers from the past all come up and let me know how beneficial the FISWG has been to them. Just knowing the FISWG has impacted them provides me with great pride and satisfaction that we have helped and continue to support the local security community."

Sal Urbano

Per the nomination package, as a DCSA industrial security representative, Urbano has always provided unparalleled service to the countless cleared defense contractors he is responsible for. He is always first in line to provide any pertinent updates, as well as in-person training sessions on the many changes that DCSA is undergoing. He has made it a mission to encourage relationships between government and industry, creating a much stronger partnership. Urbano has been paramount in seven of his facilities earning Superior ratings under the new rating matrix. He is a strong supporter and advocate for NCMS. He consistently attends NCMS local chapter meetings and communicates that attending NCMS meetings/seminars is a great resource for the industrial security community. The success of his efforts is evident by the number of government security managers who now attend industrial security meetings at contractor locations and are involving contractor facility security officers (FSOs) in the development and execution of numerous security policies and procedures implemented at their locations. Urbano encourages collaboration outside of the local NCMS chapters for those that do not have the ability to join NCMS and promotes NCMS to new FSOs. His dedication and educational guidance are greatly appreciated by the industrial security community.

The Industrial Security Award is presented by NCMS to an individual or organization that has significantly contributed to industrial security and meets a minimum of two of the following criteria:

- Individual or organization that has materially and beneficially affected the security community (i.e., functional areas include education, training, operations or like activities which improves or enhances individual, organizational or corporate performance);
- Individual or organizational contribution which improves security procedures, practices or policies of national interest (i.e., develop partnerships between industry and government, involvement in industrial security awareness councils, industry teams, etc.);
- Individual or organization continuing contributions to the Society by enhancing the mission, vision, and goals of the Society;
- A member or associate member in good standing.

DCSA Publishes Assessment of Threats to Cleared Industry

The Defense Counterintelligence and Security Agency (DCSA) Office of Counterintelligence (OCI) recently published the classified Targeting U.S. Technologies: An Assessment of Threats to Cleared Industry for cleared industry and U.S. Government partners. The unclassified companion report will be released in October. DCSA developed these publications in accordance with a Department of Defense (DOD) requirement that directs the agency to annually provide unclassified and classified all-source analyses of suspicious contacts and activities occurring within the cleared contractor community that could adversely affect the protection of critical program information.

To assist the contractor community and DoD component heads in making informed decisions to protect classified information and technology, these products provide summaries and analyses of findings on fiscal year (FY) 2022 foreign collection attempts and spotlights foreign intelligence entities' FY 2022 efforts to exploit cleared personnel or to obtain illegal or unauthorized access to classified information or technologies. The classified assessment also provides key judgments, outlooks, and intelligence gaps for threats, organized by foreign nations.

In the preface, DCSA Director William K. Lietzau states "Today, the Nation's most pressing threat comes from near-peer adversaries that target our personnel and industrial base with the goal of competing with or surpassing the United States as the premier economic and military power." He adds, "This annual assessment provides a critical lens to shape our understanding of the foreign threat to cleared industry."

Any cleared contractor interested in accessing either version can do so by reaching out to their assigned DCSA OCI Special Agent or Industrial Security Representative. In addition, the unclassified report will be available on the DCSA public website in the Reports section of the Counterintelligence & Insider Threat page.

MOVEit or Lose it!!!
Russian ransomware group exploiting newly discovered vulnerabilities

By DCSA Cyber Mission Center

Ransomware campaigns — the deployment of malware that encrypts files to deny users from accessing them and demanding a ransom to release them — are becoming more costly.

According to Chainalysis, a cybersecurity research company focused mainly on activity associated with cryptocurrency and various blockchains, within the first six months of 2023, transnational cybercriminal gangs have operated at a near-record profit using ransomware, extorting more than $449 million from their victims. The recently discovered vulnerabilities in Progress Software's MOVEit managed file transfer application could help these gangs exceed previous year's records.

MOVEit allows users to encrypt and transfer files along secured file transfer protocols. It stores consolidated files and file transfer activities in a MOVEit Cloud environment, including sensitive data like personal and proprietary information, centralized access controls, file encryptions, and activity tracking. Progress Software estimates they have thousands of federal, state, and local government organizations and business enterprises as customers using the MOVEit application, including the Department of the Army, the Department of the Air Force and members of Cleared Industry.

Oak Ridge Associated Universities and the Department of Energy's Waste Isolation Pilot Plant experienced data breaches due to the MOVEit vulnerability that impacted the personally identifiable information of potentially thousands of individuals. DCSA CMC is concerned with the specific targeting of research entities such as Oak Ridge Associated Universities. This data could later be used for further targeting of DCSA equities within the Department of Defense and Cleared Industry.

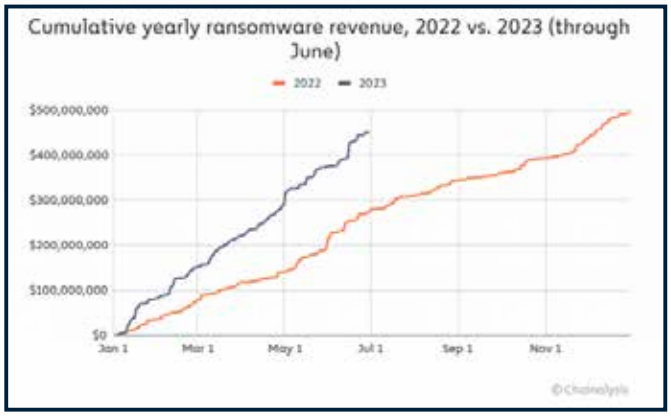
Before Progress released their software patch in early July, cybercriminal gangs launched a major ransomware campaign exploiting these vulnerabilities in MOVEit. CL0P, a Russian cybercriminal group, has claimed responsibility for the majority of the MOVEit cyberattacks.

Since the beginning of its campaign in late May, CL0P has targeted hundreds of organizations, successfully stolen data affecting more than 17 million people, and extorted some of the organizations for financial gain. An estimated $1.73 million on average has been collected per ransom.

The majority of victims were U.S.-based targets. They include public and private companies associated with aviation, transportation, logistics, entertainment, financial services, insurance, healthcare, pharmaceuticals, biotechnology, manufacturing, mechanical engineering, media, and technology sectors, the Department of Energy, and the Office of Personnel Management.

Security researchers found evidence that CL0P has been experimenting with MOVEit exploits as early as July 2021, which explains why CL0P was ready to exploit the vulnerabilities as soon as they became publicly known.

For additional information on the MOVEit vulnerabilities, see the CMC's June 6 Shared Indicator Bulletin (SIB) "DCSA-SIB-0015-23_MOVEit Transfer." The SIB highlights the technical details and provides further references. You can also contact your local Counterintelligence Special Agent. DCSA's Cyber Mission Center/Counterintelligence and Insider Threat Directorate will continue to update and distribute cyber threat information to Cleared Industry.



PAC PMO Director talks Trusted Workforce 2.0 at DCSA Fireside Chat

By John Joyce
Office of Communications and Congressional Affairs

"DCSA has the opportunity to do something really, really special in the federal government."

Over the course of an hour, Matthew Eanes – Director of the Performance Accountability Council's (PAC) Program Management Office – amplified this statement about the possibilities that no other agency, command or organization in the Department of Defense or federal government is positioned to accomplish during the third DCSA fireside chat held June 22.

He responded to multiple questions related to Trusted Workforce 2.0 and National Background Investigative Services (NBIS) posed by DCSA Employee Council member Caitlin Lerch who moderated the event as employees attended in person and virtually.

At one point, Lerch inquired, "What are you most excited about in regard to the development and implementation of NBIS - this new system of systems and what advice would you give to those who may feel some anxiety regarding the technical processes and lexicon changes this will result in?"

"I am most excited about all the future possibilities that NBIS is going to unlock," said Eanes.

The NBIS automated record checks, event-triggered activities and analysis of agency-specific information enables the Trusted Workforce 2.0 reform effort's transformation of the personnel vetting process that fully replaced periodic reinvestigations with continuous vetting of 4.4 million military, government and cleared contractor personnel.

"We changed the entire process in less than two years from a model of periodic reinvestigations that's been in place for close to 70 years," said Eanes regarding the changes made to how the government establishes and maintains trust in the workforce with a continuous risk assessment model empowered by NBIS.

"We changed the model and the way we're maintaining trust in the workforce – the entire bubble – and most of that work was done by DCSA," Eanes emphasized.

DCSA Director William K. Lietzau (right) introduces Matt Eanes, director of the Performance Accountability Council's Program Management Office, for DCSA's third Fireside Chat event held in the Russell-Knox Building at Quantico, Va., on June 22, 2023. (DoD photo by Quinetta Budd)

"Reciprocity didn't break. Access didn't break. Programs didn't break. Hiring didn't break. None of those things our new model supports, broke. The agile process allows us to do that because we quickly issued policy guidance, the implementation guidance and the reciprocity guidance."

Eanes credited DCSA – specifically, the NBIS and Vetting Risk Operations teams – for rapidly making technology adjustments and policy adjustments.

"However, it comes with the cost of ambiguity and concern and that's really hard," he reflected regarding DCSA's significant and complex role as an Investigative Service Provider (ISP) on implementing a full gamut of services on behalf of the federal government. "Change brings anxiety. There will be places where we push forward and there will be places where we take one or two steps back. Fear, uncertainty and doubt are normal human behaviors. My advice is to figure it out and have conversations with your workforce. We're all on the same U.S. government team."

Likewise, Eanes and his PAC team continuously conferred with DCSA, advising the agency on Trusted Workforce plans and policies.

The PAC is comprised of the director of National Intelligence as the security executive agent, the Office of Personnel Management director as the suitability and credentialing executive agent, the Undersecretary

of Defense for Intelligence and Security, and the Office of Management and Budget's deputy director for management as principal members. Their guidance and collaboration with DCSA resulted in the risk-reducing phased approach of Trusted Workforce 1.25 and Trusted Workforce 1.5.

Eanes told the audience that Trusted Workforce 2.0 implementation was organized into two phases. Phase One reduced a sizeable background investigation inventory and improved timeliness of investigations. Once the investigation inventory stabilized, Phase Two focused on transforming personnel vetting across the enterprise.

Phase 2a established a new vetting framework to focus on managing risk, streamlining processes and producing effective, efficient, and equitable outcomes. This framework enabled on-going development of new policies and informed Phases 2b and 2c.

Phase 2b focused on implementing Trusted Workforce 2.0 transitional states known as Trusted Workforce 1.25 and Trusted Workforce 1.5. These transitional states advanced reform and improved risk management as the new suite of Trusted Workforce 2.0 policies were under development.

In Phase 2c, the interim state transitioned to the new framework for the entire federal workforce. The new framework required finalizing the new Trusted Workforce 2.0 suite of policies to create one aligned model. Phase 2c also implemented three investigative tiers while incorporating five vetting scenarios. This effort to put the new Trusted Workforce 2.0 future state in place required changes across all aspects of the personnel vetting enterprise.

Consequently, the Phase 2 policy framework aligned the personnel vetting domains – national security, suitability and fitness, and credentialing.

Eanes also discussed how three investigative tiers implemented in Phase 2c increased processing times, reduced duplication and complexity, and improved mobility.

The transition reducing five investigative tiers to three new investigative tiers resulted in a High Tier (formerly Tiers 4 and 5), a Moderate Tier (formerly Tiers 2 and 3) and a Low Tier (formerly Tier 1).

"Now, we are in Phase 2c and transitioning into a future state," said Eanes. "This is the establishment and transfer of trust that Dr. Mark Livingston (DCSA assistant director for Personnel Security) and Heather Green (DCSA assistant director for Vetting Risk Operations) are implementing. It will all come together in the next 18 to 24 months."

The scope of Phase 2c includes finalizing the new Trusted Workforce 2.0 suite of policies to create one aligned model, implementing the three investigative tiers, and implementing the five vetting scenarios – Initial Vetting, Continuous Vetting, Upgrades, Transfer of Trust, and Re-establishment of Trust.

"Phase 2c will probably wrap up in 2026-27 as we get the scenarios rolled out," Eanes explained. "We will complete implementation over the next two and a half years and the continuing process improvement doesn't stop there. One of the things that Trusted Workforce 2.0 is providing us is future permission to do things we can't envision today."

However, changes across all aspects of the personnel vetting enterprise are envisioned to make the new Trusted Workforce 2.0 future state a reality.

"We'll have new capabilities in place that are going to unlock things that we can't even think about right now and with today's set of technologies and processes, we would never be able to do that," said Eanes. "The building blocks are being put in place for 3.0 and 4.0 in the future and this continuous learning model is a baked in component of Trusted Workforce."

One "baked in" ingredient affecting every policy in the Trusted Workforce framework features a "self-destruct" time.

"What that means is that every policy must be updated on periodicity," said Eanes. "The higher the document, the longer the periodicity before it's updated. The doctrines are updated every 5 years. The guidelines are updated every 3 years. Implementation guidance and standards are updated every year."

The model will keep pace with evolving changes in technology, process, society, data standards and availability.

"It's a self-learning model that forces the policy to change," said Eanes. "Every year we have to reaffirm each and every policy. We'll see that there's nothing to change here or say, 'here's the changes we're making.' It forces that change into the model, giving organizations like DCSA – who made a commitment to continuous learning and innovation – an opportunity and on ramps in order to influence and inform those things. Previously, there was no opportunity to do that."

Agency hosts inaugural ACE Acquisition Workforce Symposium

By John Joyce
Office of Communications and Congressional Affairs

DCSA Director William Lietzau signed the agency's acquisition instruction while opening the DCSA Acquisition Center of Excellence (ACE) at the agency's first annual ACE Acquisition Workforce Symposium, June 14.

More than 200 DCSA employees – mostly acquisition, contracting, business and finance professionals – joined Lietzau, agency leaders, and a former principal deputy director of National Intelligence at the symposium that was broadcast throughout the nation to employees attending virtually via Adobe Connect.

The acquisition instruction provides "boundaries for acquisition processes in DCSA," said Lietzau, clarifying that the signing was ceremonious since the instruction would be signed in his office to meet "mission needs on behalf of the United States of America."

DCSA, in just over 44 months since its establishment, has seen a variety of acquisition challenges. Lietzau recounted how a many of those challenges were overcome successfully as the agency continues to mature its contracting and acquisition workforce practices, processes and policies.

ACE is a community of practice that provides a centralized collaboration and tool repository hub to improve effective, efficient and innovative acquisition outcomes across the enterprise. It is a major step toward resolving some of the acquisition challenges at DCSA. Moreover, ACE will work to design and execute effective and efficient acquisition partnerships with other agencies in the Department of Defense and industry in support of mission success.

"This is about national security," said DCSA Deputy Director Daniel Lecce regarding the acquisition process and the use of ACE to impact the agency's programs such as the National Background Investigation Services (NBIS) – the federal government's one-stop-shop IT system for end-to-end personnel vetting, from initiation and application to background investigation, adjudication and continuous vetting.

DCSA Deputy Director Daniel Lecce, who also serves as the Component Acquisition Executive (CAE), explained overarching Big A Acquisition and how it relates to mission success, during the DCSA 1st annual Acquisition Center of Excellence Acquisition Workforce Symposium, hosted by the Contracting & Procurement Office and the CAE, on June 14, at the Russell-Knox Building, Quantico, Va. (DOD photo by Beth Alber)

"It's the first time something like this has been done in the federal government – the NBIS end to end system," said Lecce, who also serves as DCSA's Component Acquisition Executive (CAE). In that capacity, Lecce provides oversight and review authority for all Acquisition Programs and functions and is responsible for the acquisition workforce management and activities at DCSA. "Think about our mission statement. This is the most important thing that our nation does – national security. It's what we do and all of us have a critically important role in it every day. We've got more to do, we're going to do it, and we can't do it without you."

DCSA Contracting and Procurement Office (CPO) leaders envision that ACE will help impact the agency's mission with more "wins" by enabling improved customer and stakeholder engagement, support, repeatable processes, procedures and tools to support operations and decision documentation while providing continuous learning opportunities within the agency.

The ACE learning opportunities began at the symposium, resulting in 2.5 continuous learning points for the agency's

acquisition workforce employees engaged in briefings related to the DOD and DCSA acquisition lexicon, state of the acquisition workforce, acquisition governance, and sessions devoted to acquisition boards (Acquisition Review Board, Service Requirements Review Board, and the Contract and Agreement Review Board).

"As a fairly new agency, we are building and establishing processes while communicating how things get done," said Scott Stallsmith, DCSA senior procurement executive. "Establishing ACE – this Acquisition Center of Excellence – will go a long way to getting the message out. I envision the ACE to be a place where we're sharing lessons learned, a place where we share best practices and really try to develop what it means to be an acquisition professional here at DCSA."

In line with the DCSA Strategic Plan for 2022-2027, the establishment of the ACE advances aspects of these strategic goals – Talent, Unity of Effort, Operational Effectiveness, and Resourcing Processes, among others.

"The acquisition system goes not just to contracting," said Stallsmith. "It goes to the requirements, finances, contracts, program managers and it all culminates into a well-functioning program. In order to do that, events like this - standing up this Acquisition Center of Excellence – will go a long way in helping us mature and grow into that kind of culture we're trying to build here at DCSA."

The five goals of the ACE are to:

- Establish an integrated working group comprised of key stakeholders in the agency.
- Develop a charter that outlines the ACE purpose and scope.
- Establish a Community of Practice to identify tools and implement best practices across the agency.
- Create recognizable branding that clearly identifies ACE members.
- Work with stakeholders to ensure the required training is available, knowledge is shared across the agency, and opportunities to network are established.

"It's a team sport bringing together different disciplines of program managers, requirement writers, financial analysts,

Senior Procurement Executive Scott Stallsmith explained the role of procurement/contracting in mission success during the DCSA 1st annual Acquisition Center of Excellence Acquisition Workforce Symposium on June 14, at the Russell-Knox Building, Quantico, Va. (DOD photo by Beth Alber)

contracting officers, contracting specialists – this will be that focal point, that rallying point to bring us together," said Stallsmith. "It won't be a physical office down the hall that you can point out to where the ACE is. It will be a virtual presence with an easy to navigate website with templates and procedures and who to contact."

In other words, ACE resources and capabilities will connect myriad experts who are proactive, inspired and enabled to collaborate and provide the best acquisition services to support the agency's mission in each and every DCSA mission area – from personnel vetting, industry engagement, education and counterintelligence to insider threat support as the agency secures the trustworthiness of the U.S. government's workforce, the integrity of its cleared contractor support and the uncompromised nature of its technologies, services and supply chains.

"Do not be daunted by the processes that daunt you,"

The Honorable Sue Gordon, former Principle Deputy Director of National Intelligence, provided remarks on how vital the acquisition workforce is to achieving mission success at the DCSA 1st annual Acquisition Center of Excellence Acquisition Workforce Symposium. (DOD photo by Beth Alber)

Susan Gordon, former principal deputy director of National Intelligence, advised the audience in her keynote speech. "Rather be committed to the outcomes you must have and then work the system to be able to get there."

Gordon – who also served as deputy director of the National Geospatial Intelligence Agency – told inspirational acquisition and contract related success stories spanning three decades of her service as an intelligence officer.

"I'm honored to be here," she told a packed room of DCSA personnel before recounting policy and military strategies, decisions and lessons learned from the Cold War to the present day while briefing about how to do things, how to lead things, and how to act as an individual based on her personal experiences.

"If you're the person that is given the task to figure out how to do something and you immediately go to requirements - you have just failed the whole organization," she said, pointing out that President John F. Kennedy gave the nation and NASA a vision in 1961 about landing a man on the moon and returning him safely to earth by the end of that decade. "The first thing you must do is to envision the outcome you want and you cannot stop thinking about it until you own that outcome in your head.

The final event of the DCSA 1st Annual Acquisition Center of Excellence Acquisition Workforce Symposium featured a roundtable of speakers. In the photo, Clay Socha (center), Deputy Chief of the Contracting & Procurement Office and Head of Contracting Activity, responds to a question while Bob Jennings (left), Senior Advisor for Operations and Technology within the Chief Strategy Office, and Clyde Richards, Deputy Program Executive Officer listen. (DOD photo by Beth Alber)

Fieldwork service contracts support Trusted Workforce 2.0 initiative

Background investigations are the first step in the personnel vetting process. As the primary Investigative Service Provider for the Federal Government, DCSA conducts over two million background investigations per year on civilian and military applicants and Federal employees or employees of Government contractors and consultants to Federal programs.

DCSA's background investigations gather information on the applicant through various methods to provide a holistic picture of the applicant and provide the information needed for an adjudicator to make a determination whether to grant or deny an individual's eligibility to occupy national security sensitive positions, eligibility to access classified information, or suitability for civilian employment, fitness for selected positions, and/or credentials for access to DOD systems and facilities. Depending on the sensitivity of the position, investigative methods can include in-depth interviews with the applicant and individuals such as the applicant's current and former supervisors and co-workers, and their neighbors, and friends. The investigation also includes reviewing records pertaining to the subject, such as employment records, educational history, law enforcement and court actions, alcohol and drug counseling records, and financial records.

Part of gathering information for background investigations is accomplished via contract investigators. The new fieldwork service contracts were awarded in December 2022 to incumbents Peraton and CACI. With the new fieldwork service contractor construct, DCSA shifted from a three to two vendor model. Shortly after award, the first task orders or Notice to Proceeds were executed in April and May 2023. Since that time, all new case products have been assigned to Peraton and CACI.

The fieldwork service contracts were designed to adjust to future mission requirements that will come with the execution of Trusted Workforce 2.0/National Background Investigation Services and are worth $4.5 billion collectively. The government-wide "Trusted Workforce 2.0" initiative started in 2018 with the goals of cutting down the time needed to clear and onboard new hires, supporting reciprocity across the federal ecosystem and having the needed technology environment to enable all of that. DCSA is using this contract acquisition as a tool for its move to a new case processing system that can support more continuous vetting and monitoring of people with or applying for clearances.

New DSTC chair focusing on providing tailored learning-centric pathways

By Beth Alber
Office of Communications and Congressional Affairs

When taking over as chair of the Department of Defense Security Training Council (DSTC) in April, Heather Mardaga set goals to accomplish during her tenure. The DSTC governs oversight of DOD security certification, training, and education and also promotes and facilitates professional development for all security practitioners within the DOD.

As the DSTC chair, her role is to lead forums for DOD entities to discuss and coordinate security education and training issues and policies, recommend education and training standards and criteria, identify emerging education and training needs, and promote professional development and certification programs for the security practitioner workforce.

With that in mind, Mardaga is focused on "Improving access to security training products for Defense Security Enterprise (DSE) components personnel (users, practitioners and professionals) to provide the right level of training at the right time, and surveying the DSTC to project DSE instructor-led training seat needs for training handled by the Center for Development of Security Excellence (CDSE)."

Mardaga, who is the CDSE Director, noted that the focus of the DSTC has evolved over the years. Established in 2007, initially the DSTC focused solely on Security Professional Education Development (SPēD) certification oversight, but later broadened their focus to identifying security workforce needs and proactively leveraging the security skill standards.

She said currently, the DSTC is supporting the DSE Strategy to elevate Defense Security across the Department, Federal Government, and industry by creating a security learning framework that addresses and accommodates how components deploy their people to execute security mission responsibilities and requirements. "Specifically, the DSE Strategy is seeking to empower and professionalize the security workforce to execute its mission through enhanced and standardized security education, training, and credentialing," she explained.

"We are looking to establish a strong pathway framework," she said, "which will align a pathway for each security discipline to provide tailored learning-centric pathways for individuals to support both the enterprise and the components."

The council is comprised of senior security officials from:

- Office of the Under Secretary of Defense for Intelligence and Security (OUSDI (I&S))
- The Military Departments/Components (Air Force, Space Force, Army, Navy, Marines, and Coast Guard)
- The Pentagon Force Protection Agency (PFPA)
- The Defense Threat Reduction Agency (DTRA)
- The Defense Logistics Agency (DLA)
- The Defense Finance Accounting Service (DFAS)
- The Defense Contract Management Agency (DCMA)
- The Defense Intelligence Agency (DIA), who represents the DOD Intelligence Community Elements
- The Washington Headquarters Service (WHS), who represents the remaining Fourth Estate interests
- Public Member- DCSA Chief Strategy Office

ELDP provides better understanding of the global roles, mission of DOD

By Beth Alber
Office of Communications and Congressional Affairs

In June 2023, three DCSA employees graduated from the Department of Defense Executive Leadership Development Program (ELDP) with a better understanding of the global roles and mission of the DOD, and an understanding of the complexities and challenges of leading in a constantly changing environment.

The three employees were:

Special Agent David 'Allan' Hollenbeck, Salt Lake City (Utah) Field Office, Background Investigations, Field Operations

Edward Sanner, Trusted Workforce Implementation Management Office, Personnel Security

Special Agent Daniel Workman, Salt Lake City (Utah) Field Office, Background Investigations, Field Operations

The DCSA employees participated in the 10-month program that incorporates a multi-dimensional development approach. In total, 64 emerging leaders participated in this session, including civilians from all services, defense agencies and field activities, as well as active duty military personnel.

DCSA employees Daniel Workman, David 'Allan' Hollenbeck and Edward Sanner graduated from the Department of Defense Executive Leadership Development Program on June 9.

"I applied for the ELDP as I was looking for a more formal program for leadership development," said Hollenbeck. "It was an experience like no other."

According to the ELDP website, participants are expected to be willing and ready to step into a learning environment that may be uncomfortable, unfamiliar, and challenging—physically, mentally, emotionally, and socially. ELDP participants will be stimulated to go beyond their current paradigms and examine their assumptions, capability, and commitment to lead in uncertainty and complexity. The program leverages facilitated discussions, experiential learning activities and practical application with a focus on leading teams and understanding the complexity of DOD operations in multi-domain environments.

"The format of the training stretched me to my limits, taking me to a place that I never knew existed," Hollenbeck said. "I focused on three concepts: 1) Know yourself and what you want to become; 2) Know how to lead and make quality decisions; and 3) Know how successful DOD leaders execute their missions."

"The mix of academic studies about leadership, introspective exercises relative to one's own biases and tendencies, and experiential activities with service members and their equipment made for a balanced and self-reinforcing pattern each deployment," said Workman, noting that the learning environment was uncomfortable and challenging at times. "I was surprised in finding the strength to face my fears with some of the more physical aspects of our training. This took internal work, but really was enabled by the support of what had quickly become my trusted peers and friends from my team."

The program begins with a short orientation, followed by two weeks of Core Curriculum, which focuses on application of leadership skills through practice rather

than simple discussions and role playing. From day one, each student is thrust into leadership, team building, and followership roles through daily individual and team assignments, guided discussions, and critical thinking exercises. Students study the DOD organization and policy, practice public speaking, and prepare individual and group presentations on various DOD topics. "The opportunity was priceless. It allowed me to be stretched in countless ways to include physically, emotionally and socially," said Sanner. "It provided access and exposure to a broad set of missions across the department. It also allowed each individual to network with professionals across the department and from a variety of mission specialties."

This is followed by monthly deployments to military facilities, combatant commands, forward-deployed locations, and other government organizations to provide an overview of the DOD, and help them better understand the challenges and cultures of each of the services. During these monthly deployments, the ELDP participants experienced the military from a service member's perspective, participating in rigorous physical activities, and often sharing the same meal.

"Going into a submarine wet-trainer on our Navy deployment and having to try to fix leaks while our simulator fills with water was as stressful an event as I can think of, but I pushed through using mindfulness techniques I'd learned in ELDP and leaning on my teammates," Workman said.

Sanner noted the deployments allowed him to grow personally and professionally. "The most surprising discovery was how 'short' my limits were," he said. "As I have traveled my journey, along the way I had built many limitations for myself. To be stretched beyond those limits was refreshing, inspiring and encouraging. I intend to leverage that experience as I continue in my professional career."

Now that the ELDP experience is behind them, all employees indicated they wouldn't hesitate to recommend the training to other DCSA employees.

Sanner noted, "To the individual that is driven and self-motivated and has a strong desire to learn and grow and a passion for professional leadership development, I would recommend this training without hesitation."

"I would highly recommend this program to everyone," said Hollenbeck. "If you're looking to see why you can't grow or find promotion? This program will help you find success…not just with work, but in your personal life as well."

"To be able to do important self-work, to practice what you've learned in a leadership laboratory traveling the world, and to meet the warfighters across all branches and types of service was a once-in-a-lifetime opportunity," Workman said. "Beyond personal growth, the development of networks across 22 different DOD agencies will prove invaluable as participants move into positions of leadership throughout their careers."

Edward Sanner, Background Investigations, sits in a 25th Combat Aviation Brigade UH-60 medevac helicopter at Wheeler Army Air Field, Hawaii.

Daniel Workman, Field Operations, finishes a one-rope bridge crossing across the Yellow River at Eglin Air Force Base, Fla., as part of a 'swamp walk.'

CDSE holds conferences to address needs of, inform security community

By Samantha Dambach
Center for Development of Security Excellence

Each year, the Center for Development of Security Excellence (CDSE) hosts three different conferences on behalf of DCSA to address the needs of the security community. This year, all three of the conferences were virtual, which not only allowed for larger audience participation, but also saved on TDY costs and allowed those stationed overseas to attend.

The first conference was the Virtual DCSA Security Conference for Industry (vDSCI) which took place on April 26 and 27. The theme was "Elevating Industrial Security" and featured speakers throughout DCSA discussing the Facility Clearance Process, How to Run a Successful Self-Inspection, Cyber Hygiene, CI Reporting, Insider Threat, and Personnel Security. Both days ended with panel discussions where the over 2,000 attendees were able to ask speakers questions in real-time.

The second was the Virtual DCSA Security Conference for DOD (vDSC-DOD) held on August 16 and 17, with the theme "Elevating Security through Vigilance and Innovation." This conference had speakers from DCSA, Under Secretary of Defense for Intelligence and Security, DOD Inspector General, and Navy. The speakers discussed the Secretary of Defense directed "45 Day Review" of security programs, policies, and procedures; Personnel Vetting; Security Executive Agent Directive 3; Personnel Vetting; Insider Threat; CI Threat Trends Medical Devices and the DOD; and Policy Updates. The vDSC-DOD had 2,730 attendees over the two days. If you missed any sessions or would like to re-watch, you can get links for the recorded sessions on the CDSE Webinars and

Conferences, https://www.cdse.edu/Training/Webinars-and-Conferences/.

Lastly, the Virtual DCSA Conference for Insider Threat was on September 7, as part of National Insider Threat Awareness Month (NITAM). This conference featured insider threat practitioners in DOD, federal agencies, private industry, critical infrastructure sectors, and academia to support the 2023 NITAM theme of "Bystander Engagement." The discussed counter-insider threat professionalization, organizational resources, toolkits for insider threat mitigation, and more. The recorded sessions will be available on the CDSE Webinars and Conferences, https://www.cdse.edu/Training/Webinars-and-Conferences/.

A group of government and industry stakeholders selected the topics and themes for each conference.

CDSE received a lot of great feedback from the conferences:

"*[Being an FSO] is great job but it is hard to do it alone. We need to synch together in order to better protect our clear industry and US government. Thank you for this event." – vDSCI participant*

"Great information on SEAD 3 reporting; very straightforward" – vDSCI participant

"Excellent presentation and ADOBE Connect was a tremendous success as the platform for this conference. Looking forward to future presentations." – vDSC-DOD participant

"As a new member to this field outside the military, all of these presentations were very beneficial." – vDSC-DOD participant

Defense Counterintelligence and Security Agency

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil

571-305-6562

www.DCSA.mil