

Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper



Volume 4, Issue 3



**ASK THE LEADERSHIP:
DAVID CATTLER**

**DCSA PRESENTS
COGSWELL AWARDS**

**IN THIS ISSUE
LEADERSHIP OF
PEO CHANGES**

IN THIS ISSUE

FROM THE DIRECTOR	3
DAVID CATTLER FORMALLY TAKES HELM AS DCSA DIRECTOR	4
DITMAC, U.S. NAVY APPLY NEW COUNTER INSIDER THREAT CAPABILITIES VIA SITH	9
DCSA RECOGNIZES THE BEST IN INDUSTRIAL SECURITY; 14 FACILITIES RECEIVE COGSWELL AWARDS IN 2024.....	12
AGENCY PRESENTS EXCELLENCE IN COUNTERINTELLIGENCE AWARDS; DCSA EMPLOYEES RECEIVE NCMS INDUSTRIAL SECURITY AWARDS	14
LEADERSHIP OF PEO CHANGES, PART OF CONTINUED AGENCY TRANSFORMATION	16
FIELD OPERATIONS ENHANCING NATIONAL SECURITY THROUGH INTEGRATION	18
IMPROVING THE CUSTOMER EXPERIENCE: DCSA'S ROLE AS A HIGH IMPACT SERVICE PROVIDER.....	20
DCSA ADVISORS ASSIST JAPAN WITH DEFENSE INDUSTRIAL SECURITY MANUAL, MISWG MEMBERSHIP	21
NEW DCSA DIRECTOR FOCUSES ON FUTURE CAPABILITIES AT INSIDER THREAT FORUM.....	25
NEW ONLINE COURSE SEEKS TO REDUCE INSIDER THREAT RISKS	28
UNTREATED MENTAL HEALTH CONDITIONS POSE SECURITY RISKS	31
"ONE PS:" UNIFIED MISSION STRENGTHENS PERSONNEL SECURITY	33
REGIONAL SUMMIT STRENGTHENS INTEGRATION OF MISSIONS, OUTLINES WAY FORWARD	35
CI CHIEF OF STAFF GAINS VALUABLE EXPERIENCE AT WHITE HOUSE DETAIL	36
NHL TEAM HONORS DCSA SECURITY MANAGER AS HOMETOWN HERO	38

Vol 4 | ISSUE 3

DCSA Gatekeeper

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

DCSA LEADERSHIP

David M. Cattler
Director

Juli MacDonald
Chief, OCCA

Cindy McGovern
Managing Editor

Elizabeth Alber
Editor

John J. Joyce
Dante Swift
Staff Writers

Christopher P. Gillis
**Digital Content
Specialist**

Craig Richardson
**Layout, Editing and
Design**

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

All pictures are DOD photos, unless otherwise identified.



FROM THE DIRECTOR

I am just marking my first 100 days as the Director of DCSA. The first 100 days of a presidential term has taken on symbolic significance, and the period is considered a benchmark to measure the early success of a president. The term harkens back to the first 100 days of Franklin D. Roosevelt's presidency when he signaled his intention to move with unprecedented speed to address the problems facing the nation in his inaugural address.

I have taken a different approach in my first 100 days at DCSA. I have spent as much time as possible listening and learning and there is a lot to learn about DCSA. You can see that in the articles reflected here from an ongoing collaboration with the Japanese government to DITMAC's outreach to the insider threat community. Our mission is extensive and it's exciting.

I made it an early priority to meet with key stakeholders across DOD, the federal vetting enterprise, and cleared industry. I have spoken at multiple events, sharing my background and direction for the agency. In each speaking event, I shared the idea that security is a team effort; we are all in this together and facing the nation's security challenges demands nothing less.

There are some issues that required my immediate attention, most notably the National Background Investigation Services or NBIS. By the time this edition is published, I will have formally testified at two Congressional hearings on our management of NBIS. I want to stress what I said at both hearings: we are fully committed to delivering a federal IT system to enable the personnel vetting mission.

DCSA will move forward with a program that instills confidence, a program that delivers capabilities to uphold mission without fail. I am confident in our path forward and expect to be held accountable. We've embraced collaboration with our oversight partners and together we will take NBIS on a sustainable pathway forward to ensure a trusted workforce, to protect the Nation and earn and secure the public's trust.

I share more of my initial thoughts in this edition's "Ask the Leadership."

Thank you for your continued support of DCSA.

A handwritten signature in black ink that reads "Dm Cattler".

David M. Cattler
Director,
Defense Counterintelligence and Security Agency

David Cattler formally takes helm as DCSA Director

By John J. Joyce

Office of Communications and Congressional Affairs

QUANTICO, Va. – David Cattler's assumption of the Defense Counterintelligence and Security Agency (DCSA) directorship was formally recognized at a ceremony held at the National Marine Corps Museum on May 29, 2024.

"I am thrilled to have you aboard leading our nation's Gatekeepers during this next chapter of DCSA," said the Honorable Milancy Harris, Acting Under Secretary of Defense for Intelligence and Security, in her keynote speech while reflecting on Cattler's extensive military and civilian experience.

"You're taking the helm at a pivotal moment," Harris told Cattler as more than 250 guests – including former and current senior Department of Defense officials, congressional staff and industry executives – joined DCSA leaders and workforce as well as Cattler's family and friends to witness the official assumption of directorship.

"Your team has been planning and executing transformative efforts since DCSA was created," said Harris, who officiated the ceremony. "I'm proud of the work they've done, mindful of what's ahead, and excited to see what will be accomplished under your leadership."

After her remarks, Harris presented the Under Secretary of Defense for Intelligence and Security medallion to Daniel Lecce, for distinguished service while fulfilling simultaneous roles as DCSA acting director and deputy director from Sept 28, 2023, to March 24, 2024.

"I personally appreciate the stability, consistency, honesty and transparency you provided to I&S and to the DCSA workforce during the interim period between directors," said Harris while presenting the award to Lecce, who continues serving DCSA as the agency's deputy director. "Dan launched a nationwide unity of effort roadshow designed to listen to the workforce and hear their concerns firsthand. By addressing these concerns and being proactive, Dan's actions ensured DCSA continues to be an employer of choice."

Immediately after the award presentation, the moderator read Secretary of Defense Lloyd Austin's orders appointing Cattler as the director of DCSA. Harris presented Cattler with the certificate of commission, signed by Austin, appointing him as the new DCSA director with all the privileges and authorities appertaining to the office subject to the conditions prescribed by law.

In his remarks Cattler noted the attendance of Director of National Intelligence Avril Haines. "I'm honored you're here," said Cattler. "You're a terrific leader of the intelligence community and in the international community of intelligence and security services. I'm proud to count you as a mentor and a friend."

Cattler also acknowledged others in the audience to include former Naval Academy classmates, intelligence and security agency directors, senior executives, and key stakeholders such as Matthew Eanes, director of the Performance Accountability Council's Program Management Office within the White House Office of Management and Budget.



Acting Under Secretary of Defense for Intelligence and Security Milancy Harris (left) passes the DCSA flag to Director David Cattler, while Chief of Staff Ellen Ardrey watches on during an Assumption of Directorship ceremony held May 29 at the National Museum of the Marine Corps, Quantico, Va. (DOD photos by Christopher P. Gillis)

Cattler also shared why he was excited to lead an agency focused on security and counterintelligence after his many years of service in the intelligence community.

"I learned a lot about security while I was in NATO, especially that I needed to learn more about security," said Cattler who previously served as assistant secretary general for intelligence and security at NATO.

Cattler's 20 years of experience in national security and intelligence also included leadership positions as assistant director of National Intelligence and chairman of the National Intelligence Management Council within the Office of the Director of National Intelligence.

"There's so much to appreciate and so much advantage in focused and purposeful integration between intelligence and security," he explained. "It's a real advantage for both missions.

"Security is about trust," he emphasized. "We try to understand the threat and come up with ways to address these threats and manage the risks that they pose from a security perspective." Cattler reflected that since he interviewed for the position as DCSA director, he has come to learn "how significant, how broad and how deep our security roles actually are."

The agency's integrated security mission focuses on personnel security, vetting, industry engagement and security education in addition to counterintelligence and insider threat support. This focus enables DCSA to secure the trustworthiness of the United States government's workforce, the integrity of its cleared contractor support, and the uncompromised nature of its technologies, services, and supply chains throughout the country.

"I couldn't do my job in the intelligence community without superb security. I wouldn't know what to trust and I might not be trusted myself," said Cattler. "At DCSA, we advance and preserve America's strategic edge by ensuring a trusted federal and industrial workforce and enabling industry's delivery of uncompromised capabilities."

At one point, Cattler spoke directly to DCSA civilian, military and contractor personnel – known as America's Gatekeepers who safeguard the nation by providing a trusted workforce and protecting the industrial base.

"I jumped at the opportunity to serve as your director. Why? Security really matters, always, and especially now," he said. "I will listen and learn from you. I will fight to remove any barriers preventing you from being successful. I will fight for the resources you need to do the job you need to do. I will help you ensure that we bring the best of DCSA's capabilities and our partners' [capabilities] to bear to protect and enhance our national security."

The ceremony gave Gatekeepers the opportunity to formally welcome their new director while providing Cattler with the opportunity to share the moment with Charles Phalen and Daniel Payne, the directors of DCSA's legacy organizations.

"Thank you for your farsighted vision and hard work," said Cattler. "You led and shaped many of the people who currently serve at DCSA."



Acting Under Secretary of Defense for Intelligence and Security Milancy Harris (left) presents DCSA Deputy Director Daniel Lecce with the Under Secretary of Defense for Intelligence and Security medallion for distinguished service during an Assumption of Directorship ceremony held May 29 at the National Museum of the Marine Corps, Quantico, Va.

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.

David M. Cattler is the Director of the Defense Counterintelligence and Security Agency (DCSA), the United States Government's premier provider of integrated security services, effective March 24, 2024. DCSA is a strategic asset to the Nation and its allies—ensuring a trusted federal and industrial workforce and enabling industry's delivery of uncompromised capabilities. DCSA uniquely blends industrial security, counterintelligence support, personnel vetting, and security training to advance and preserve America's strategic edge. He leads the agency's strategic transformation and maturation, and a workforce of approximately 12,000 federal and contract support personnel worldwide.

Before joining DCSA, Mr. Cattler served as Assistant Secretary General for Intelligence and Security at the North Atlantic Treaty Organization (NATO), and informed and protected NATO decision-making. He helped form and coordinate national policy as Deputy Assistant to the President for Regional Affairs within the National Security Council. He was a senior advisor to the Director of National Intelligence in multiple roles, including Chairman of the National Intelligence Management Council, National Intelligence Manager for the Near East, and Principal Deputy National Intelligence Officer for Military Issues. He supported combat operations while directing the Defense Intelligence Agency's counterterrorism efforts and serving as the Joint Staff's Deputy Director for Intelligence.

He began his career as a naval surface warfare officer and served in two Aegis cruisers, USS ANTIETAM and USS CHANCELLORSVILLE, and ashore in military and civilian roles with the Office of Naval Intelligence and Director of Naval Intelligence.

He has earned academic degrees from the U.S. Naval Academy and Georgetown University. He also is a graduate of the National Intelligence University, the U.S. Naval War College, and was a senior fellow at the Massachusetts Institute of Technology's Seminar XXI.

QUESTIONS AND ANSWERS

We have your biography and you've introduced yourself to the workforce and to industry. Is there anything in your background that you would like to highlight or reinforce?

Everyone has access to my biography so I won't belabor that. But I would like to share a bit about my career. I think, and this is particularly true of my time at NATO, that I learned enough about security to know that I didn't know everything I needed to know. I want to learn and continue to grow and that's one thing that really interested me about this job.

I want to be better for my time at DCSA than I was when I came in and I want the agency to be better as well. So, I'm learning every day; I'm picking up on things that are being discussed, that are getting done, getting redirected, you name it. I really approach this job from the lens of an analyst; fact based, methodical and unemotional.

I've served at all the staff levels all the way up to the White House. I have been the lead oversight official for the DNI or the director of a key combat support agency at multiple levels in those chains of command. I share that because over the course of my career, I've gotten to know a lot of people with the Intelligence Community, DOD, and beyond. And having those shared experiences is very beneficial to this position. We've had a lot of the same formative experiences and as a result, we hold the same values to be really important. We've learned the same lessons, some good, some bad, and we tend to approach the problems the same way. Why is that helpful? Because when you're working under high pressure or when things are not going well, we have a common understanding and, quite frankly, some good will in the bank. As the new guy, I can start from a position of friendship and trust and that is a huge advantage.

You've stated that being Director of DCSA was something that you sought out. What made you interested in the job?

I gained a great appreciation for the value of security during my time at NATO. I was integrating multiple intelligence and security services for the NATO enterprise and had to deal with real security problems regularly. Security is critical to our ability to manage and mitigate risks. It helps build trust in the system—trust in our workforce, trust in our facilities, and trust in our systems that data, technologies, capabilities will be protected, and we will be able to maintain our competitive edge. We need security services to also promote the safety of the workforce—Insider threat capabilities help detect violent, dangerous, and potentially lethal actions before they happen. We need security services to protect our intelligence and decision—making space. So I see the value of security and I understand how important trust is to the Intelligence Community. You have to be able to trust that your intelligence is accurate and uncompromised and security provides that assurance.

I am also very interested in the DCSA mission and its future. I think this is a unique time in our country. We are facing adversaries that will use any means possible to exploit our technological and manufacturing advantage. And that advantage is what will prevail on the battlefield and it is absolutely critical that we, the United States and our allies, prevail.

Directors often come into the role with an overarching objective. What are your main objectives for your tenure at DCSA?

I have laid out three key goals for the agency:

- **Recognized as world class security provider and preferred partner:** Establishing the agency as the recognized premier provider of integrated security services and the preferred partner in the security services mission space.
- **Operating at full performance:** Ensuring the agency is operating at full performance across all missions—after five years of consolidation and transformation we need to move beyond the start—up phase. The public and our stakeholders have a number of reasonably high expectations for the agency and we need to be delivering on them in full.
- **Futureproof:** Preparing the agency to execute its missions into the future. I am challenging the DCSA team to look at 2040 as a benchmark. I am asking “What will the threat and mission environment look like and how must we adapt?”

I want to push us to consider our future—what opportunities and challenges will there be? What new data sources will be available? How can that data be exploited? How will our work change? What should DCSA look like and be able to do in that future? What will the threat environment look like and how will perform in it? The bottom line is, the workload, the missions, the requirements, and the risk are not likely to decrease.

I've said in several forums that I want to look at everything we do. I don't say that to scare people, but we have to be honest about the fiscal environment we're living in. We can't just increase the number of dollars and people we have and keep asking for more. It's not sustainable. So we need to think about efficiencies and how we can better leverage our existing resources.

Since its inception in 2019, DCSA has been through significant transition and transformation. Do you see more such change on the horizon or has the agency settled into an organizational/operational structure.

It's been five years since the agency's formation and in my short time here, I see a unified DCSA ready to fully avail ourselves of the functions that came together to create the agency. I'm not one to come in, shake up the puzzle pieces and rearrange them. It's not healthy and it causes too much uncertainty. And quite frankly, as I said, I don't think that's needed at DCSA. But in general, I am very engaged with the leadership team and many of our external stakeholders to help understand the current state of DCSA and where we are in our journey. We may need to, over time, make some marginal changes, but each of the core missions that we have personnel, security, industrial security, CI and insider threat and security training, they're great. That's the right mix. The priority varies, the resourcing varies, but each of our core mission elements are important. To deliver our missions in a world class way, we need a world class support team and I think we have that as well. Everyone who works for DCSA, no matter where they sit, no matter what they're doing is helping us move into the future and achieve these mission outcomes.

In the short time you have been Director, what has been your most pleasant surprise?

I don't know that it was a surprise, but I am most taken by the length of service and depth of expertise of the workforce. We have a workforce with incredible experience and depth of understanding of our mission. I have individuals who are recognized experts in the community. When I talk about world class performance, it relies on a world class workforce and we have that at DCSA.

Conversely, what have you identified as your most distressing surprise?

Again, I'm not sure I would classify this as a distressing surprise, but I wasn't prepared for the amount of IT development and maintenance the agency manages. It's not just NBIS, but also DISS, BIES, eApp, PDT, NISS, NCCS, SITH, DSOS. That's a lot of IT for an agency that isn't an IT agency. Adding to the challenge is the importance of these systems. When you're responsible for a system of record for the entire American cleared population, that's sobering.

I came to DCSA clear-eyed about NBIS; about the challenges with delivery and opportunities that it brings when the capability is implemented. And we've been working alongside our DoD oversight partners and have coordinated a 90-day recovery plan to move NBIS forward.

For all of these systems, we're looking at everything: the right people; the right agile processes; the right relationship with oversight; and the right responses, advice, and recommendations.

You have made engaging with industry, stakeholder, Congress a priority. What kind of feedback are you hearing and how are you incorporating that feedback into your guidance to the agency.

My first goal is to establish the agency as the recognized premier provider of integrated security services and the preferred partner in the security services mission space. One way to do that is to increase our engagements with industry senior leaders, our government customers and stakeholders and our Congressional overseers. I am doing that and I am gathering feedback.

You made publishing your Director's Intent a priority and shared your thoughts at your first townhall. How has that message been received by the leadership and have you had any feedback from the workforce?

I think this is important but with every new director, there is angst: What is he like to work for? How does he want to receive information? Change is hard. So I wanted to quickly and clearly articulate how I want the agency to operate.

My goal with formally publishing my Intent was to define how we should expect each other to operate to accomplish our mission. I want all DCSA employees to hold each other to high standards to accomplish our critical national security mission. We are a unified community of security professionals that choose the hard right over the easy wrong. We should be audacious and ambitious in improving the way we execute our mission.

Is there anything else you would like our readers to know?

I am incredibly proud to be leading the DCSA team. This is an agency of remarkable people who are serious about their work. The reasons we do this work matter – standards matters – living up to our national security mission matters – holding people to these standard matters. Too many times recently have individuals dumped the nation's secrets and exposed crucial sources and methods to our adversaries. If our corporate cultures don't address the seriousness of what we do – realize our collective role, then no Gatekeeper anywhere will be able to prevent bad outcomes.

We have a vision statement that points to some very simple concepts "... national security is our mission and people are our greatest asset..." This is something I have seen from our workforce and I want all of us, in this collective mission space to never forget the crucial role each of us has in protecting our nation's security and the lives of our military. Thank you.

DITMAC, U.S. Navy apply new counter insider threat capabilities via SITH

By John Joyce

Office of Communications and Congressional Affairs

QUANTICO, Va. – The onboarding of insider threat professionals from the U.S. Navy and the Department of Defense (DOD) Insider Threat Management and Analysis Center (DITMAC) into a new technology called the Solution for Insider Threat Hindrance (SITH) is just the beginning of an extensive DOD onboarding process, according to Defense Counterintelligence and Security Agency (DCSA) officials.

In all, 72 counter insider threat professionals from the Navy and DITMAC are managing unclassified insider threat cases in SITH – an interim solution while DITMAC System of Systems (DSoS) Increment 2 is under development.

“We are genuinely excited about deploying SITH to the insider threat community. It took a monumental group effort to get this project across the finish line as a new solution in the hands of our users,” said Shannon Walters, DITMAC DSoS deputy program manager at the DCSA Program Executive Office. “SITH demonstrates DCSA’s ability to deliver solutions that meet the needs of our customers – making their jobs more efficient and providing new features that will have a positive impact on the mission. SITH is a real win for DCSA and the insider threat community. Its success built confidence in our ability to continue delivering capability with Increment 2.”

The SITH interim solution introduces Prevention Assistance and Response (PAR) program functionality for DITMAC and case management capabilities for the PAR cadre at the installation level and insider threat component hubs. In addition, SITH maintains the existing DSoS Increment 1 capabilities for managing and analyzing insider threat information.

DSoS Increment 1 – still in effect for DOD users pending migration to SITH – is a unique custom built enterprise level capability for managing and escalating insider threat information.

Overall, the DSoS mission supports DOD components, sustainment of technologies that aid in the management, analysis and mitigation of insider threat information in support of the DOD Counter Insider Threat Program Strategic Plan, DITMAC, and the DOD Insider Threat Program Implementation Plan.

The newly established PAR program relies on its coordinators assigned to military bases across the country who advise commanders and base leadership in the prevention, assistance and response to potential threats. SITH functionality and management features are already enhancing PAR coordinators’ efforts at gathering information to include a holistic assessment of an individual or threat in order to make recommendations that will raise awareness, assist leadership decision making, and help prevent and reduce risk.

“SITH and our work towards DSoS Increment 2 is an absolute game changer as we move forward to building a scalable DSoS that works for the entire insider threat community, including the PAR program” said Challenge Gray, DITMAC program manager for SITH.

DSoS also serves as the insider threat community’s primary tool for capturing, consolidating, storing, analyzing and managing insider threat data reported to the DITMAC. It supports 54 insider threat hubs and programs—43 DOD and 11 civilian—on the Secret Internet Protocol Router Network (SIPRNet) and the Joint Worldwide Intelligence Communications System (JWICS) highly secure communication networks used by the U.S. government and military to share classified information.



“SITH and our work towards DSoS Increment 2 is an absolute game changer as we move forward to building a scalable DSoS that works for the entire insider threat community, including the PAR program.”

*—Challenge Gray,
DITMAC Program Manager for SITH*

SITH, however, tracks and manages insider threats that exist on the Non-Classified Internet Protocol Router Network (NIPRNet) to allow the insider threat hubs to ingest, triage, manage and escalate incidents as they are identified.

“This NIPR capability is fantastic since a majority of our cases are on the unclassified side,” said Gray. “It will allow everybody to perform their jobs to the best of their abilities a lot quicker and smoother as well as that cross coordination—allowing each component to talk to one another and coordinate on such a higher level than they currently are able to.”

Moreover, the SITH product provides initial capabilities encompassing enterprise case management, continuous vetting, continuous evaluation, alert ingestion, sharing closed cases, basic reporting and role—based dashboards.

“SITH is the first major steppingstone as a standalone implementation bringing us to the next phase—DSoS Increment 2,” said Erin Lambert, DSoS program manager at DCSA’s Program Executive Office. “DSoS Increment 2 will eventually provide data automation and integration with other systems, enabling us to send our data to other systems.”

Lambert described her team’s collaboration with user communities as a “hand in hand” operation to develop a SITH solution that works technically to enable future expansion and scalability.

“Our unique partnership and coordination with the user community was vital to get to where we are in the development of SITH,” she said. “We’re moving in the right direction to deliver functionality the insider threat user community will find beneficial for the mission as we continue with SITH deployments and the transition to Increment 2.”

DITMAC officials envision DSoS Increment 2 as a broad—based capability that supports installation—level reporting, support for the DITMAC PAR program, user access monitoring, and behavioral threat analysis capability. It will feature adaptation to allow for automated data ingest to directly support and enhance analytic efforts focusing on areas of increased risk. DSoS Increment 2 includes development efforts for automated data ingest by adding additional data sources and the addition of reporting, analysis and data visualization capabilities.

The SITH good news was outlined chronologically in Lambert’s April 15 email to DCSA leaders and teams who helped make the interim SITH solution to DSoS Increment 2 a reality.

She pointed out that the DCSA Decision Authority established SITH as a prototype on March 29, 2023. It was followed by the agency’s Acquisition Review Board’s February 1, 2024 authorization to deploy SITH to the Navy, DITMAC and the DCSA Operations Analysis Group.

“Since then, the team completed planning and execution activities necessary to operationalize SITH for the Insider Threat mission,” Lambert recounted. “These activities included user testing, independent verification and validation testing, cyber and regression testing in addition to user training, building out of the production environment, obtaining an Authority to Operate, establishing the help desk, creating user guidance and documentation, and onboarding preparations.”

In her announcement about the product’s development and onboarding process, Lambert emphasized that SITH is the first DCSA solution hosted on the newly established Impact Level 5 National Security Cloud ServiceNow SaaS architecture, introducing NIPR level functionality to the insider threat community.

DOD Impact Level 5—encompassing controlled unclassified information (CUI) and unclassified national security information—is used to host non-public, unclassified national security system data or non-public, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. This includes CUI and other mission data that may require a higher level of protection than was afforded by IL4 as deemed necessary by the information owner, public law or other government regulation.

Meanwhile, the software acquisition and procurement planning phase for DSoS Increment 2 continues as the gradual onboarding of SITH takes place throughout the DOD insider threat community until December 2024.

The development phase of DSoS Increment 2 is planned to start in fiscal year 2025 with its minimum viable capability release scheduled by the end of that fiscal year with multiple integrations to follow in fiscal year 2026.

DSoS Increment 2 will be self—hosted at DCSA, eventually providing users with access to NIPR IL—5, SIPR and JWICS domains. Its functionality, incorporating everything within the capability assessment, will deploy incrementally via Agile releases to include full functionality for case management and PAR requirements.

Lambert concluded her email report by crediting internal and external partners in the consultation and collaboration process resulting in a “truly monumental accomplishment that would not have been successful without the efforts and support of multiple teams and partners among government, federal contractor and internal DCSA partnerships.”



“SITH is the first major steppingstone as a standalone implementation bringing us to the next phase – DSoS Increment 2.”

*—Erin Lambert,
DSoS program manager at DCSA's
Program Executive Office*

DCSA recognizes the best in industrial security; 14 facilities receive Cogswell Awards in 2024

On June 12, 2024, the Defense Counterintelligence and Security Agency presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 14 cleared contractor facilities, during the annual NCMS training seminar in Nashville, Tenn. The Cogswell awards represent the “best of the best,” and the winning facilities’ security programs stand as models for others to emulate. These 14 facilities represent less than one—tenth of one percent of the approximately 12,500 cleared facilities in the National Industrial Security Program (NISP).

“It’s clear that any time we can get this many FSOs [facility security officers] and other experts together; it’s not just a win for the participants but for the entire security enterprise,” said DCSA Director David Cattler during his remarks. “Many in the audience are FSOs...you are where the rubber meets the road. What you do matters. What we do together in our NISP [National Industrial Security Program] mission is important.

“Security is about enabling and protecting the ability of the United States to maintain a decisive advantage,” the director continued.

To qualify, companies must establish and maintain a security program that exceeds basic National Industrial Security Program requirements. Recipients also help other cleared facilities establish security-related best practices while maintaining the highest security standards for their own facility.

The Cogswell Award selection process is rigorous. A DCSA industrial security representative may only nominate facilities that have at a minimum two consecutive superior industrial security review ratings and which show a sustained degree of excellence and innovation in their overall security program management, implementation and oversight. DCSA makes the final selections.

Established in 1966, the award honors Air Force Col. James S. Cogswell, the first chief of industrial security within the Department of Defense. Cogswell developed the basic principles of the Industrial Security Program, which includes emphasizing the partnership between industry and government to protect classified information. This partnership provides the greatest protection for U.S. warfighters and our Nation’s classified information.



DCSA Director David M. Cattler provides keynote remarks during the NCMS 60th Training Seminar and later presented certificates to the winners of the DCSA Cogswell Awards, Nashville, Tenn., June 12, 2024. (DOD photo by Christopher P. Gillis)

Congratulations to the 2024 Cogswell Award winners!



Adapt Forward, LLC
Charleston, S.C.

CAMO LLC, a LinQuest Company
Beavercreek, Ohio

Iridium Satellite LLC — Tempe
Tempe, Ariz.

Leonardo DRS – Naval Powers Systems, Inc., Danbury, CT
Danbury, Conn.

Lockheed Martin Aeronautics – Skunk Works
Palmdale, Calif.

Lockheed Martin Government Affairs, Yorktown, VA
Yorktown, Va.

Lockheed Martin Logistics Services, Inc., Greenville, SC
Greenville, S.C.

MZA Associates Corporation
Albuquerque, N.M.

PeopleTec, Inc.
Huntsville, Ala.

Phoenix Global Support, LLC
Fayetteville, N.C.

Raytheon Cyber Solutions, Inc.
Annapolis Junction, Md.

TechGuard Security, LLC
Scott Air Force Base, Ill.

Teledyne Defense Electronics, LLC – dba Teledyne e2v HiRel Electronics
Milpitas, Calif.

The Aerospace Corporation
Colorado Springs, Colo.

Agency presents excellence in counterintelligence awards; DCSA employees receive NCMS industrial security awards

During this year's annual NCMS training seminar, Janet Banzer, Industrial Security, Field Operations, and Timothy Schroeder, Adjudication and Vetting Services, received NCMS Industrial Security Awards for 2024. DCSA also presented the John "Jack" F. Donnelly Awards for Excellence in Counterintelligence to five entities.

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.

Janet Banzer

Per the nomination submission, Banzer goes the extra mile to ensure that industry can meet mission success. She is willing to work together to develop solutions that ensure compliance while addressing the needs of the businesses that she supports. She not only provides the guidance, but she also walks the process and procedures step by step, creating a clear and concise path to success. Banzer, who is the New York Field Office Chief, has fostered and provided guidance to many experienced and new facility security officers under her purview. She creates an environment of inclusive partnership that spans across her entire team. She takes every conversation or site visit and turns it into an opportunity for growth and development.



DCSA provided 10 different helpdesk booths in support of the NCMS 60th Training seminar, Nashville, Tenn., June 11, 2024. (DOD photos by Quinetta Budd)

She is always willing to listen to the needs of industry and supports creative solutions to complex issues. She invites out of the box thinking and listens to industry concerns. Whenever called upon to provide support for the local NCMS chapter for meetings or providing responses to industry questions, she is the first to raise her hand and show support to industry. She has provided templates for sharing and explains in detail a path to success, providing education to FSOs and senior management officials.

Timothy Schroeder

Per the nomination package, when you attend the NCMS Seminar and go to the Adjudication and Vetting Services (AVS) Helpdesk, Schroeder is the guy back in the office that is making all the adjudicative actions happen. Over the past several years, he has served as the focal point of contact for NCMS to assist in the update of cases. Since November 2023, he has assisted in the cases of 150+ where we called him directly for assistance. An “unofficial partnership” was developed with Schroeder, and he has been receptive and reactive in receiving the applicable cases and working them going above and beyond to obtain updates for the facility security officers. His timely assistance has helped many NCMS company missions, allowing the clearances to adjudicate in a timely manner and individuals to access the information they need to perform the services needed.

Developing an “unofficial partnership” with Timothy, NCMS benefits from his responsiveness and dedication. He ensures cases receive the necessary attention, often providing updates within days, even during weekends. Timothy's efforts facilitate timely clearances and access to essential information, supporting NCMS company missions effectively. His prompt assistance has proven invaluable in expediting cases that had been stagnant, enabling individuals to fulfill their roles efficiently.

Excellence in Counterintelligence Awards

Also announced during the NCMS seminar, the FY23 John “Jack” F. Donnelly Award for Excellence in Counterintelligence recipients were announced. This award is presented annually to cleared contractor companies and academic institutions that have exhibited outstanding accomplishments in preventing the theft of sensitive or classified U.S. information and technology by foreign entities. This award not only recognizes their achievements, but also encourages all cleared entities to maintain superior counterintelligence programs that contribute directly to national security. The selection process for this prestigious award is similar to the rigorous process for selection of the James S. Cogswell Award. It involves a panel that carefully reviews nominations from counterintelligence special agents, who put forth exceptional candidates from seven cleared corporations and academic institutions.

The recipients of the FY23 Jack Donnelly Award for Excellence in Counterintelligence are:

AM General LLC

Carnegie Mellon University – Software Engineering Institute

Lockheed Martin Corporation

Michigan Technological University -- Keweenaw Research Center

Virginia Polytechnic Institute and State University

These organizations showcased the most impressive counterintelligence capabilities and demonstrated exceptional cooperation with the U.S. government in deterring, detecting and disrupting the theft of sensitive or classified U.S. information and technology by foreign entities.

Leadership of PEO changes, part of continued agency transformation



DCSA Director David Cattler (left) executes the Assumption of Charter for the new Program Executive Officer Edward Lane during the PEO Charter Ceremony, May 21, at the National Museum of the Marine Corps, Triangle, Va. (DOD photos by Christopher P. Gillis)

DCSA Director David M. Cattler presided over the Program Executive Office Change of Charter ceremony on May 21, 2024, presenting the charter to the new PEO Edward Lane, and Lane in turn conferred charters on Robert Schadey, National Background Investigation Services executive program manager, and Dennis Lujan, Publicly Available Electronic Information program manager.

In 2019, the deputy secretary of defense directed the transfer of several information technology acquisition programs to DCSA. The new mission required an acquisition capability to oversee the diverse IT development programs transitioning from across the federal government. The acquisition capability would need to achieve milestones and monitor costs to avoid volatile increases in budget requirements while delivering the best technology to help secure the U.S. government's technologies, services, and supply chains. The entity was the PEO, formally established on Oct. 1, 2020.

"The PEO oversees a portfolio of enterprise-wide information technology programs and within our agency, that's eight programs altogether within the portfolio.," said Cattler. "With the formulation of the PEO, we have a capability within our agency to deliver a range of world class enabling tools to the people that are engaged in a broad range of missions whether it's personnel security, industrial security, counterintelligence, insider threat or security training. There are elements of those eight program offices under the PEO that support all those critical missions."

In presenting the charter to Lane, Cattler said, "Ed brings a lot of highly relevant experience and knowledge. I have full trust and confidence in Ed leading the PEO and I'm honored to present a well-deserved charter to him today."

Prior to joining DCSA, Lane was the Defense Intelligence Agency's (DIA) Deputy Senior Acquisition Executive. He was the senior advisor on program and contract management for the DIA acquisition enterprise where he provided resource management and programmatic guidance across the Office of the Chief Information Officer (OCIO), including the Department of Defense Intelligence Information System and Joint Worldwide Intelligence Communications System communities.

In accepting the charter, Lane outlined his commitment to excellence and the way forward.

"The PEO team must be professionals who are fully trained and certified," he said. "We need to be innovative and look for new methods and new ideas to support the mission. We need to employ good governance, make sure as a team we're ensuring consistent and transparent execution of our baseline, and finally, we need to be culturally proficient, working together, embracing diversity, and adopting shared values."



Program Executive Officer Edward Lane (left) executes the Assumption of Charter for the Executive Program Manager for the National Background Investigation Services (NBIS) Robert Schadey during the PEO Charter Ceremony, May 21, at the National Museum of the Marine Corps, Triangle, Va.

"I look forward to delivering and sustaining the current DCSA operational baseline," he continued, "and helping design the future security architecture that takes full advantage of modern technology."

Lane then executed the Assumption of Charter for Schadey as the executive program manager for NBIS.

Prior to joining DCSA, Schadey was responsible for integrating and modernizing the Army's enterprise resource planning systems, focusing on enterprise initiatives such as cloud migration, cloud computing, and data analytics.

"It is an honor to accept the formidable and crucial responsibilities of steering the National Background Investigation Services system," said Schadey after accepting the charter. "This program is more than a series of procedures and protocols. It is a foundational pillar of our nation, of our nation's security and trust infrastructure. Every day, countless individuals entrust DCSA with their most personal

information and we must safeguard that trust with the utmost integrity, precision, and vigilance. The diligent and thorough execution of these responsibilities depends on the essence of our national security, the integrity of our public institutions and the safety of our industrial base.

"I am deeply aware of the gravity of this role and the stakes involved," he continued, "and I'm committed to maintaining the highest accuracy, confidentiality and efficiency standards in background checks."

Lane then executed the second Assumption of Charter for Lujan as the program manager for PAEI.

Lujan has served as a Senior Portfolio/Program Manager for the U.S. Army, Department of State, Veterans Health Administration, and Environmental Protection Agency, where oversaw several initiatives such as the Integrated Acquisition Program, Construction Management, Software Integration and Business Process Improvements.



Prior to DCSA, he was with the Information Resource Management Bureau in the Department of State which provided innovative, effective, and interconnected diplomacy by constantly improving, modernizing, and refreshing various tools and services while protecting information and IT assets against cyber threats and vulnerabilities.

"I stand before you not as a program manager, but as someone deeply committed to harnessing technology to drive meaningful change and innovation within our agency," Lujan said.

Program Executive Officer Edward Lane (left) executes the Assumption of Charter for the Program Manager for Publicly Available Electronic Information (PAEI) Dennis Lujan during the PEO Charter Ceremony, May 21, at the National Museum of the Marine Corps, Triangle, Va.

Field Operations enhancing national security through integration

By Dante Swift

Office of Communications and Congressional Affairs

As the premiere provider of integrated security services, the Defense Counterintelligence and Security Agency is uniquely postured to bolster National Security. In the evolving threat landscape, the need for continuous integration and collaboration across DCSA is paramount. Using a thorough and proactive approach, the Mid-Atlantic Region of Field Operations, along with Personnel Security (PS) and the Counterintelligence and Insider Threat Directorate, coordinated a pilot program with the strategic purpose of increasing mission integration across mission elements in the field and with directorate level offices.


At the heart of the Mission Integration Pilot Program is a centralized integrated team, aimed at fostering collaboration and creating repeatable processes within the agency. At its core, the program seeks to unify mission efforts across PS, Counterintelligence (CI), Background Investigations (BI), Cybersecurity (CS) and Industrial Security (IS) through the creation of standardized processes, while mitigating risks and ensuring a cohesive approach to safeguarding national interests.

One of the key objectives of the program was to break down authorities and operational processes that often hinder communication efforts and information sharing. A primary outcome of this effort was the development of processes that resulted in the cross-mission Integrated Element (IE) receiving shared case information when the analysis of the DCSA Form 521s (Investigations Threat Operations Group/ITOG Referral Form) indicated a higher-risk case was present and “need-to-know” was clearly established. This resulted in the IE prioritizing actions based on mission authorities. The DCSA Form 521 is utilized by BI Special Agents when a threat is identified during a personnel security background investigation and captures case identifying information and specific details regarding the identified threat. The IE is comprised of representatives of BI, IS, CS, and CI, and a Regional Action Officer. In coordination and conjunction with the Integrated Review Team (IRT), the IE serves as the focal point for Field actions in this pilot. The IE coordinates region-specific activities with the IRT for awareness, feedback, and/or any other associated actions pertaining to the 521 referrals for the Mid-Atlantic Region. The IE is also responsible for ensuring integration occurs within the appropriate mission areas in the region in accordance with established information sharing procedures, as directed per Privacy, Civil Liberties Office, Office of the General Counsel, and Intelligence Oversight Office.



“In addition to actions taken on specific cases, one of the pilot benefits has been building the foundation for integration, both from a process and culture perspective, that will ultimately enable the agency to utilize mission authorities, operations, and data to better inform the threat picture across Industry and the federal enterprise.”

-Justin Walsh
Mid-Atlantic Region Director

An abstract graphic at the top of the page features a dark blue background with a faint, stylized globe. Overlaid on the globe are white circuit-like lines with small circles at the nodes and arrows indicating a flow or direction. The lines are more prominent on the left side and fade towards the right.

By utilizing best practices, expertise, and resources, the pilot participants were able to optimize collaboration while staying ahead of emerging threats and challenges in an increasingly complex security landscape.

Being proactive instead of reactive to risk management and mitigation, has served as a catalyst for robust threat assessments and information sharing among Field Operations and with directorate level offices. The pilot program enables security experts to anticipate and address challenges before they escalate and initiate cross-mission information sharing sooner. Exercising a case triage methodology, CI specific and pertinent information was communicated to the Mid-Atlantic field missions to further prioritize actions that could be taken by all four missions in a unified approach to mitigate potential risk to classified technology/programs. These actions included targeted threat briefings, information sharing on facility security posture, greater insights into SEAD 3 compliance and adversary methods of contact and operations being used at specific facilities.

"In addition to actions taken on specific cases, one of the pilot benefits has been building the foundation for integration, both from a process and culture perspective, that will ultimately enable the agency to utilize mission authorities, operations, and data to better inform the threat picture across Industry and the federal enterprise," said Justin Walsh, Mid-Atlantic Region director.

As the security landscape continues to advance, initiatives like this pilot will play a critical role in safeguarding national interests. While the functional benefits and the key takeaways provide in-depth clarity on areas of improvement, the Mission Integration Pilot fostered a sense of unity and shared purpose.

"Conducting this pilot has made the four Mid-Atlantic missions a stronger unified team focused on both short-term and longer-term actions," said Katharine Kolwicz, Deputy Regional Director (Integration), Mid-Atlantic Region. "Employing the expertise of professionals with diverse backgrounds and disciplines, while promoting a culture of teamwork results in a renewed sense of what it means to be a Gatekeeper of national security."

At the conclusion of the pilot, all partners will develop proposed courses of action to further standardize mission integration opportunities and unity of effort.

The Mission Integration Pilot Program represents a paradigm shift in how the agency can approach security challenges. DCSA is working toward a more integrated and effective national security processes by fostering collaboration in identifying and mitigating risk to futureproof agency operations.

Improving the customer experience: DCSA's role as a High Impact Service Provider

In December 2023, the Office of Management and Budget designated the Defense Counterintelligence and Security Agency as a High Impact Service Provider (HISP). Federal organizations are selected due to the scale and critical nature of their public-facing services that have a high impact on the public. There are currently 38 Federal entities designated as a HISP. "Being designated as a HISP is testament to the far-reaching critical mission our agency performs," said Deputy Director Daniel J. Lecce.

Why are HISPs so important? The number two priority of the President's Management Agenda (PMA), released on Nov. 18, 2021, is to deliver excellent, equitable and secure Federal services and customer service. Specifically, to improve the customer experience management of HISPs by reducing customer burden and streamlining processes. As stated in the PMA, "Every interaction between the government and the public is an opportunity to deliver the value and competency Americans expect and deserve."

Due to the complexity of the personnel security clearance application process and high volume of personnel security clearances (which includes over 100 Federal agencies and cleared industry under the National Industrial Security Program), DCSA has designated its HISP service area of focus as customer engagements and support during the initiation/application phase of the personnel security clearance application process.

DCSA is committed to meeting its HISP requirements in conducting comprehensive assessments of the initiation/application phase of the vetting application process, measuring customer experience maturity, and identifying actions to improve support. This includes creating action plans which outline a strategy for improving the customer experience and streamlining existing processes to attain identified goals. In addition to the overarching goal of improving the customer experience, other identified goals include increasing confidence and trust in DCSA during the application/initiation portion of the personnel security clearance process, while increasing customer understanding of the requirements necessary to complete an application.

To achieve these goals, DCSA's action plans will outline service delivery enhancements which will include providing customers with educational material pertaining to the vetting application process as well as improvements to the dcsa.mil website to provide clearer guidance and easier navigation. DCSA will measure enhancements to customer experience through feedback mechanisms (such as surveys) strategically built into the personnel security clearance process to highlight improvements and identify areas for further focus. DCSA will provide enhancements to the dcsa.mil website and deploy customer feedback surveys in FY25. Enhancements will include robust informational personnel security clearance-related products and other high-quality touchpoints with customers. Following implementation of these items, DCSA will continually review results from the surveys and based on the feedback received, make further improvements to customer experience.

"It is the policy of the United States that, in a Government of the people, by the people and for the people, improving service delivery and customer experience should be fundamental priorities" -- EO 14058, "Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government," signed by President Joseph Biden on December 13, 2021.

DCSA advisors assist Japan with Defense Industrial Security Manual, MISWG membership

By John Joyce

Office of Communications and Congressional Affairs

TOKYO, WASHINGTON and QUANTICO, Va. – Defense Counterintelligence and Security Agency (DCSA) industrial security professionals collaborating with their Japanese counterparts at home and abroad, directly impacted the inaugural publication of Japan's Defense Industrial Security Manual (DISM), leading to its membership in the Multinational Industrial Security Working Group (MISWG).

As the first Asian nation to become a member of the MISWG – Japan joined Australia, Austria, Israel, Switzerland and NATO member nations in the non-governmental organization that develops common security procedures for the protection of classified information shared under non-NATO Multinational Defense Programs and international industrial security matters.

"Japan did this – it's all of their effort, and we appreciated the opportunity to advise, assist and share our security practices on the industrial security side to help inform their industrial security policy. The publication of the Defense Industrial Security Manual is really a cornerstone that set the stage for Japan's security program moving forward," said Jennifer Skelton, Technology Security and Foreign Disclosure Division deputy chief at the Defense Technology Security Administration (DTSA). "The DISM is really critical and postured Japan well for their MISWG membership given the stringent criteria to become a MISWG member."

As the government's experts in international information sharing, information security and technology security, safeguarding the U.S. technological edge while enhancing foreign partners' capabilities, DTSA is the U.S. government lead for the Bilateral Information Security Consultations (BISC).

This includes consultations with Japan regarding its industrial security program. Skelton and Scott Nelson, deputy assistant director for the DTSA International Engagement Division, needed the highest level of industrial security expertise for this BISC line of effort and knew who to contact for support: DCSA's Industrial Security Directorate headquartered in Quantico, Va.

DCSA industrial security experts immediately responded to the DTSA request for assistance, engaging as advisors in support of Japan's efforts to meet substantial equivalency with the U.S. National Industrial Security Program (NISP) and the strict MISWG criteria.

The NISP ensures that cleared U.S. defense industry, more than 12,500 facilities, protects classified information in their possession while working on contracts, programs, bids or research and development efforts.

The BISC—formed as a result of a 2009 U.S.-Japan summit meeting—launched a series of consultations to strengthen security cooperation, including information security that deepens the U.S.-Japan Alliance. The BISC fosters a government-to-government dialogue on information security essential to fully enabling the 2007 U.S.-Japan General Security of Military Information Agreement (GSOMIA), which governs the reciprocal protection of classified information.

This continual dialogue includes collaborative BISC engagements impacting Japan's national security in the wake of its MISWG membership in May 2023 and official visits between Japanese Prime Minister Fumio Kishida and U.S. President Joe Biden. The latest meeting, held at the White House on April 10, 2024, celebrated a new era of U.S.-Japan strategic cooperation.

"We continue to deepen our cooperation on information and cyber security to ensure that our alliance stays ahead of growing cyber threats and builds resilience in the information and communication technology domain," Biden and Kishida announced in their joint statement. "We also plan on enhancing our cooperation on the protection of critical infrastructure."

DCSA industrial security professionals Dan Finucane and Monica Son recalled the March 2023 DTSA request to support the U.S.-Japan BISC third line of effort focused on cooperation in the industrial security domain, which comprises technology, information, cyber, personnel and physical security. Japan's industrial security leaders completed a draft of their DISM—similar to the National Industrial Security Program Operating Manual (NISPOM)—and just finished translating it from Japanese to English. At that point, three of the agency's senior industrial security subject matter experts—Son, Finucane and Kevin Williamson—engaged a new BISC mission: Review Japan's DISM and collaborate with its authors via virtual meetings and correspondence while providing feedback and advice based on years of industrial security experience, expertise and knowledge.

"We had a finite amount of time to review Japan's industrial security plan of actions and milestones as well as their Defense Industrial Security Manual," said Son in reference to the government of Japan's anticipated release date three months later. "Recognizing the importance of the BISC and its potential long-term impact on expanding defense technology cooperation between the United States and Japan, our team ensured this effort remained as a high priority until its completion."

Finucane, DCSA Industrial Security Field Office chief in the Mid-Atlantic Region, and Son, a senior industrial security representative based in the agency's Western Region were also preparing for two trips to Japan for in-person consultations related to the DISM and its implementation during visits to Japan's cleared defense contractors.

However, the review, consultation and collaboration process on Japan's DISM needed to be completed first.

"Our goal was to gain an acceptable level of understanding of the Japanese industrial security program and their systems of checks and balances in order to sufficiently provide our comments and recommendations back to Japan in a timely manner," said Son. "It was evident our foreign partner was extremely committed to ensuring the DISM was as comprehensive and comparable to the NISPOM as possible based on how responsive and receptive they were to our feedback. The intent throughout our collaborations was to standardize and ensure substantially equivalent information security practices between the United States and Japan."

Now that the virtual consultations were complete, the duo traveled to Tokyo in August 2023, coinciding with Japan's admittance to MISWG and its publication of the DISM.



"It was evident our foreign partner was extremely committed to ensuring the DISM was as comprehensive and comparable to the NISPOM as possible based on how responsive and receptive they were to our feedback. The intent throughout our collaborations was to standardize and ensure substantially equivalent information security practices between the United States and Japan."

-Monica Son
Senior Industrial Security
Representative, Field Operations

Meanwhile, Hideki Tsuchimoto – Japanese Ministry of Defense (JMOD) commissioner of the Acquisition, Technology and Logistics Agency (ATLA) – released his statement, introducing the DISM publication.

“ATLA has now formulated the Defense Industrial Security Manual, which is equivalent to the industrial security programs and operation manuals of other countries,” said Tsuchimoto. “The DISM is a document which unifies information protection measures implemented in the defense industry based on laws, regulations, rules etc. concerning the protection of classified information that applies to the defense industry. ATLA will distribute the DISM to the defense industries in Japan and share it with the governments and defense industries of the ally and like-minded countries to strengthen defense production and technology bases, including international equipment and technology cooperation.”

Moreover, the ATLA website described its DISM as a publication that “unifies information security measures based on laws and regulations in order to increase transparency and reliability of Japan’s defense industrial security as well as to contribute to defense equipment and technology cooperation.”

Tsuchimoto’s team of industrial security officials welcomed the U.S. delegation to Japan as the DISM was distributed to the nation’s defense industries.

Specifically, the U.S. contingent comprised representatives from DTSA, DCSA and the F-35 Lightning II Joint Program Office (JPO). The F-35 JPO leads the life-cycle program management of the F-35A, F-35B, and F-35C: the fifth-generation joint strike fighter air system of choice for the U.S. Air Force, U.S. Navy, U.S. Marine Corps, international partners and foreign military sales customers.



“We received very detailed briefings from each company about their security practices and procedures. It was an excellent chance to observe and view Japanese industry and focus on industrial security and how it’s been implemented. There were certain areas that were absolutely beyond substantial equivalency. In fact, we found some best practices that we would certainly take back to our industry.”

*-Dan Finucane
Field Office Chief, Hanover 2 Field Office*

U.S. Embassy personnel from the Mutual Defense Assistance Office (MDAO) also attended various meetings and site visits throughout the two trips. The agenda included a tour, briefings and a security review with discussions at Japanese defense contractor facilities.

“The DISM’s implementation and the broader concept of substantial equivalency with U.S. industrial security and the NISPOM was our focus,” said Finucane. “We saw exactly how industrial security was implemented at cleared contractor facilities in and around Tokyo and we observed several examples of substantial equivalency first-hand. Japan’s industrial security program, in many aspects, is very similar to the U.S. program. We also saw how the DISM was received, viewed and implemented by those Japanese companies.”

The DCSA team walked throughout defense contractor facilities and plants while observing and engaging with Japanese corporate officials and employees, asking questions and sharing best practices. “It was really impressive, and, in some ways, it seemed that we were conducting security reviews of U.S. cleared contractors in the NISP,” said Finucane. “We received very detailed briefings from each company about their security practices and procedures. It was an excellent chance to observe and view Japanese industry and focus on industrial security and how it’s been implemented. There were certain areas that were absolutely beyond substantial equivalency. In fact, we found some best practices that we would certainly take back to our industry.”

Finucane continued describing his experience touring seven Japanese cleared defense contractors during visits in August 2023 and February 2024.

“We were pleased to find really strong practices in the physical security lane of industrial security and documentation was very strong,” he said. “As we go through the BISC industrial security line of effort in concert

with DTSA, I'm really optimistic that that we're going to keep finding more and more substantial equivalency and being able to move toward saying that overall – Japan has met that mark for industrial security.”

As the industrial security line of effort comes to a close, the U.S. and Japan are planning to engage in efforts to enhance Japan's security education and training program for their security workforce. DCSA Center for Development of Security Excellence representatives will provide information to Japan's training professionals related to security education, training and professionalization for DOD and industry under the NISP.

“Over the past five years – through BISC, GSOMIA and our relationship — there has been so much growth benefiting Japanese defense programs as well as U.S. defense programs and cleared industry supporting our national security efforts as well as their own,” said Richard Stahl, DCSA International and Special Programs chief. “The amount of work accomplished has been tremendous and due to the efforts of our personnel visiting Japan but more importantly, due to the effort and seriousness in the Japanese development, enhancement and implementation of its personnel and industrial security programs.”

The last five years Stahl refers to involves DTSA's second line of effort under BISC. It comprises bilateral efforts that began in September 2019 as DCSA Personnel Security leaders advised and assisted Japan with its security clearance background investigation and adjudications programs. This second line of effort, which concluded in 2024, ensured that Japan's access to sensitive U.S. government information meets U.S. information security and personnel security standards. The same is true of U.S. access to Japan's sensitive government information. This substantial equivalency is crucial to ensuring that information shared between the U.S. and Japan remains secure.

In all, U.S.-Japan BISC collaboration centers on the following five lines of effort aimed at strengthening information security practices between the two nations.

- Designating a National Security Authority for Japan – first line of effort concluded in 2020.
- Background Investigations/Security clearances – second line of effort closed in 2024.
- Industrial Security – on-going. Milestone accomplishments include Japan's publication of their DISM and MISWG membership.
- Security Professionalization – DCSA looks forward to assisting Japan's efforts to strengthen its security education and training program for its security workforce.
- Classified Information in Courts – the Department of Justice is the lead for this future bilateral effort, centered on how classified information should be handled during the course of investigations and in the Japanese court systems.



“The amount of work accomplished has been tremendous and due to the efforts of our personnel visiting Japan but more importantly, due to the effort and seriousness in the Japanese development, enhancement and implementation of its personnel and industrial security programs.”

—Richard Stahl
DCSA International and Special
Programs Chief

New DCSA director focuses on future capabilities at insider threat forum

ARLINGTON, Va. – Defense Counterintelligence and Security Agency (DCSA) Director David Cattler challenged 160 insider threat professionals to describe their vision of Department of Defense (DOD) insider threat capabilities as he kicked off the “Insider Threat Analyst Forum” on April 8.

“Let’s chart our course today,” said Cattler, responding to his challenge regarding the future of DCSA and its oversight of the DOD Insider Threat Management and Analysis Center (DITMAC).

He then shared his vision – emerging technologies to include mining and analyzing data with AI and machine learning will significantly impact prevention and mitigation of future insider threats to national security.

“Think about 2040 – what does that future look like,” Cattler inquired in his first speaking engagement since assuming responsibility as the agency’s new director on March 24. “Where will we be?”

The former assistant secretary general for intelligence and security at NATO asked deeper questions while inspiring attendees representing more than 30 DOD insider threat components, ranging from intelligence community elements to military services and combatant commands.

“What opportunities and challenges will there be,” he asked participants at the two-day inaugural event. Cattler continued with inquiries about DITMAC’s future: What new data sources will be available to perform most roles? How can that data best be exploited? How will our work change as a result of that environment, the data, and new tools?

“We had to separate the wheat from the chaff or find a needle in a haystack,” Cattler explained regarding data analysis in times past. “The problem today is that all of the data is useful. So much of it is so good, that you have a harder time trying to pick out which pieces are the most important and which pieces of that haystack of needles are the most useful to help you solve the problem you’re dealing with. That’s where we need to get you better technology and as computing technology – especially AI – becomes better developed, we should be able to better exploit these data sources to improve our mission, performance and outcomes.”

Data analysis is one of myriad tools DITMAC uses to identify, assess, and mitigate risk from insiders, to oversee and manage unauthorized disclosures, and to integrate, manage, mature, and professionalize insider threat capabilities.



DCSA Director David Cattler provides keynote remarks during the DOD Insider Threat Management and Analysis Center Insider Threat Analyst Forum on April 8. (DOD photo by Christopher P. Gillis)

Insider Threat analysts look for insights and data to understand what risk factors are present and what mitigation options can be considered from a threat management perspective. They work to contextualize reports received from DOD component Insider Threat hubs by identifying any predispositions, stressors, patterns of behavior, or additional concerning behaviors that may be present in an individual.

Cattler referred to a specific case reported to DITMAC by a DOD Insider Threat Component about an individual whose behavior met insider risk criteria under several DITMAC reporting thresholds.

“All of the employee’s behaviors and incidents add up to what most analysts would say is a pattern. And the pattern is disturbing but the good news is that this case is an example of collaboration and information sharing at its best,” he recounted. “Based on a notification from a force protection referral to an insider threat hub and subsequent submission to our DITMAC team, the insider threat was mitigated. Connecting the dots across DOD and with our federal partners is the key to success.”

This highly collaborative approach is necessary to holistically address the risks associated with an insider threat.

“That’s just one recent great example of this community represented here today coming together in action,” said Cattler. “When people see something and say something and consequently, when we do something together in a timely fashion, there’s a greater chance that we can mitigate risks early and protect our national security.”

The process begins as DOD Insider Threat components report cases to DITMAC if an individual’s behavior meets the criteria under one or more reporting thresholds. DITMAC’s case management system enables information sharing across the insider threat enterprise. DITMAC analyzes the reported incident and provides recommendations for mitigation. At that point, insider threat component hubs implement mitigation recommendations that DITMAC oversees to final resolution.

“Early identification of these risks and enabling mitigating action is vital to security and safety,” Cattler emphasized. “You’ve got a vital mission to protect our information systems, facilities and people. You could be preventing real violence that could lead to people being hurt or killed.”

From initial report to resolution, DITMAC’s parallel and complementary role with DOD components in the handling of specific incidents is vital to early mitigation of insider risks. The role features DCSA analytic experts who evaluate relevant insider threat data; generate findings and risk assessments; and provide recommendations for components to mitigate the insider threat. Components submit insider threat matters to DITMAC when incidents meet specific reporting thresholds.

There are 13 DITMAC reporting thresholds: serious threat; allegiance to the United States; espionage and foreign consideration; personal conduct; behavioral considerations; criminal conduct; unauthorized disclosure; unexplained personal disappearance; handling protected information; misuse of information technology; terrorism; criminal affiliation; and adverse clearance actions.

“Insider threat is a team sport and I recognize the critical role that we all play in building trust through our partnership – each and every day – while ensuring national security and helping to keep people safe,” said Cattler. “Our insider threat program can enable us to detect a potential threat, intervene early, and to get the individual help they might need. The example I described resulted in the removal of that individual, but there are a number of examples resulting in people getting help and reestablishing trust relationships with the government. This makes DITMAC an incredibly strong partner and force—multiplier for many leaders across the total force.”

DCSA’s posture to help mitigate risks from trusted insiders across the DOD enterprise starts with the agency’s Personnel Security mission, which includes Background Investigations and the Continuous Vetting service.

“We also have a team here from our Adjudication and Vetting Services or AVS. Ask them good and really hard questions about that process,” Cattler suggested to participants. “The vetting world and insider threat are closely tied together, and they really do need to hear from you — they need that information.” This risk mitigation process concludes with adjudicators at AVS who determine security clearance eligibility of non-intelligence agency DOD personnel occupying sensitive positions or requiring access to classified material including sensitive compartmented information.

Among those in attendance were Prevention, Assistance and Response (PAR) coordinators who are using 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 joint bases or regions and service specific military installations.

As they provide assistance, PAR coordinators work closely with functional experts resident on the installations to ensure military and civilian leaders have the information necessary to assess and manage risk. The ultimate goal is to provide an individual the appropriate resources, such as financial planning, marriage counseling or employee assistance programs, to mitigate future risk of a violent or destructive act.

Experts from DITMAC's Behavioral Threat Analysis Center (BTAC) were also participating and presenting briefs to include a presentation called 'Understanding Risk with Suicide and Domestic Violence.' The multidisciplinary team is impacting DOD with case—specific insider threat recommended mitigation strategies in behavioral science, threat management, cyber, counterintelligence, law enforcement and human resources.

Their influence began sweeping across DOD when BTAC was formed as an emerging capability in fiscal year 2023 following the Countering Extremism Activities Working Group recommendations directed by the Secretary of Defense. The new mission area is integral to supporting DITMAC's ability to mitigate emerging and evolving insider threats by leveraging its expanded and new capabilities.

DITMAC key programs include Analysis and Mitigation capability to consolidate and share information necessary to identify potential insider threats, develop a holistic picture of risk posed by insiders, and coordinate actions to mitigate risk across DOD. The Mission Integration Office supports enterprise User Activity Monitoring efforts and integrates Publicly Available Information into insider threat analytic products to contextualize risk.

A breakout session at the event involved a discussion with DCSA Security Training and the agency's Center for Development of Security Excellence (CDSE) on Insider Threat Analyst Training Needs Analysis.

CDSE is the premier provider of security training, education, and certification for DOD, federal government, and cleared contractors under the National Industrial Security Program. CDSE provides development, delivery, and exchange of security knowledge to ensure a high—performing workforce capable of addressing the nation's security challenges.

"Our training team helps to set and implement standards for important security related credentials to ensure that our teams are properly trained and ready for their work no matter which organization they serve," said Cattler. "Looking to the future I consider that our current DCSA strategy is good to enable a sustained high performance. However, we've got to take advantage of these new computing capabilities so that we can keep the humans involved with the things that we need to do while cued by the computer. It means that the computer will tell you where there are anomalies; to go through the very large quantities of data that we have, and tell you what it thinks it sees that does not quite make sense. Then you can intervene, take a look at it, and help the system – whether it be Insider Threat program, AVS, or other mission partners. Take the cue that could be based on a computer tip and see what it leads to."

New online course seeks to reduce insider threat risks

By Allison Wolff

DOD Insider Threat Management and Analysis Center

The Gatekeepers of the Defense Counterintelligence and Security Agency (DCSA) are committed to protecting America's national security information by developing and expanding the online training curricula offered by the Center for Development of Security Excellence. This effort includes the Insider Threat Detection Analysis Course (ITDAC), specialized curricula for insider threat operations personnel and management personnel respectively, as well as the newly developed, in-person Department of Defense (DOD) Insider Threat Analyst Forum. Through these initiatives, DCSA strives to provide timely and relevant content that is easy to understand and will help build a strong, knowledgeable cadre of insider threat professionals within the community.

The ITDAC is a five-day online analytic course, currently open and available for registration as part of the Center for Development of Security Excellence's (CDSE's) virtual instructor-led offerings. Another DOD agency previously hosted the course, but it has recently transitioned to be included among the CDSE's repertoire of offerings. With the ITDAC, analysts from across the insider threat community can attend and grow their skills to support their respective insider threat programs while simultaneously building a network of personnel with shared interests.

"Insider threat detection and analysis is important because insiders can cause considerable harm to an organization's sensitive data, intellectual property, financial stability, or even the safety and well-being of its employees," explains Robin White, DOD Insider Threat Management and Analysis Center (DITMAC) Professionalization Lead. "With the growing number of insider threats and advanced cyber-attacks, organizations require insider threat professionals with specialized skills and knowledge in identifying and mitigating these threats. This type of training improves organizational security posture and reduces the risks associated with insider threats."

The ITDAC teaches insider threat analysts to apply critical thinking skills and analytic techniques to identify potential insider threat indicators. Other objectives include:

- Applying policy, Executive Orders, and DOD and Intelligence Community authorities to gather holistic data while ensuring constitutional and privacy rights are maintained.
- Determining the appropriate processes for conducting and reporting insider threat response actions from intake of an initial potential threat to mitigation of the threat.
- Assessing the procedures for disclosing mandated counterintelligence and criminal activity information to the appropriate agency or office.

During the course, students work to complete five practical exercises in areas such as: misuse of information technology, potential workplace violence, espionage, mental health, and continuous evaluation.

"Insider threat detection analysis courses are an essential aspect of professionalization, enabling insider threat professionals to develop the knowledge and skills necessary to identify and respond to insider threats effectively," says White.

Before arriving, analysts attending ITDAC must have successfully completed the Insider Threat Program Operations Personnel Curriculum or the Insider Threat Program Management Personnel Curriculum. Both tracks and associated pipelines are available and managed by the CDSE's insider threat training team run by Amber Jackson. "CDSE provides security education, training, and certifications for DOD and industry under the National Industrial Security Program (NISP)," said Ed Kobeski, branch chief of counterintelligence and insider threat with CDSE. Now, CDSE is focused on updating their extensive online library of insider threat resources and integrating content with the latest advancements

in technology, policy, and best practices throughout the government and industry. Resident CDSE experts collaborate with DCSA insider threat professionals from the DITMAC to make sure that the resulting curriculum is functionally sound and relevant to the community's needs.

DITMAC is responsible for identifying, assessing, and mitigating risks from potential insider threats across the Defense Enterprise, managing unauthorized disclosures, and integrating, managing, maturing, and professionalizing insider threat capabilities. DITMAC's experts supported the ITDAC transition by providing content guidance and resources to assist in the development and delivery of the training.

DITMAC's Assessment and Professionalization (A&P) team focuses on insider threat professional development, methodologies, and standardization. They provide guidance to other Insider threat programs to support growth, effectiveness, and efficiencies. This expertise complements CDSE's training mission, ensuring DCSA provides a unified product to their customers.

In addition to the online offerings, this April, DITMAC hosted its inaugural Insider Threat Analyst Forum. It expanded on concepts and objectives discussed and developed in ITDAC. DITMAC provided guidance on advancements within the insider threat community by hosting experts to discuss processes, case studies, and professional development.

"This being the first DOD forum of its kind, we see that as an opportunity for sharing information, discussing processes, and building a network you can rely on for years. The very small communities across intelligence, security, and insider threat can only benefit from the partnerships fostered here," explains James Shappell, DITMAC director.

In addition to professionalization, DITMAC's A&P team performs site visits to provide the DOD insider threat programs guidance on compliance with the National Insider Threat Task Force (NITTF) standards and recommendations to enhance the effectiveness and efficiency of the programs. The team conducts a plethora of surveys, interviews, and observations to build a thorough report to the organization it is supporting. This exposure enables the A&P team to stay current on insider threat community's developments and acquire best practices for dissemination across the community.

"DITMAC amplifies the voice of the community by sharing and integrating their feedback into the training courses, conferences, and webinars that the DITMAC supports," articulates Mark Burns, chief of A&P team. "We have a strong



relationship with CDSE. They assist by providing the community a standardized curriculum to build depth and strength within their insider threat programs.”

CDSE’s strengths are further complimented by DITMAC’s expertise to propel the insider threat curriculum as the best in class among insider threat professionals. These training programs include over 70 case studies, and CDSE’s extensive insider threat materials also include eLearning courses, 45 job aids, 47 security posters, tool kits, and training videos.

ITDAC satisfies training requirements for personnel assigned to insider threat programs identified in the Presidential Memorandum of November 21, 2012 — National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. The policy referred to in this memorandum mandates the following trainings for insider threat personnel: Counterintelligence and security fundamentals, insider threat response, laws, regulations, civil liberties, and referral requirements.

“ITDAC provides a baseline knowledge,” said Burns. “The Analyst forum and tailored DITMAC onsite insider threat program assessments continue to build on that baseline and provide each program with additional knowledge, services, and capabilities. We [DITMAC] want to continue to be the premier authority on Insider Threat programs and support.”

Previously, National Insider Threat Task Force and DITMAC partnered with DIA’s Joint Military Intelligence Training Center to provide a virtual insider threat analysis course, which has since been reviewed, revamped, and updated. ITDAC, the current version, is available to federal insider threat program analysts from the DOD, the Intelligence Community, and non—title 50 communities. ITDAC provides insider threat analysts the ability to apply critical thinking skills and structured analytic techniques to address potential insider threat indicators at no cost.

“CDSE builds reliable content aligned to current policy, course objectives, training standards, and the insider threat community’s operational applications,” said Kobeski.

Shifting to the DOD’s ITDAC comes following the rise of a new Global Counter Insider Threat Program Certification from the University of Maryland. This program, developed in conjunction with DCSA and the OUSD (I&S) is available to government and industry partners and aligns to the standards first developed for the Certified Counter—Insider Threat Professional programs.

“Ensuring the entire community has the ability to receive a standard of insider threat training is paramount,” said Shappell. “Our industry partners need the ability to grow and develop their insider threat programs to further a holistic approach and support the interconnectedness of the insider threat problem set.”

Untreated mental health conditions pose security risks

By Dante Swift

Office of Communications and Congressional Affairs



On May 7, 2024, more than 300 agency employees convened virtually to engage in a discussion that illuminated the intersection of mental health and national security. The virtual gathering served as guidance to participants who were eager to understand the nuances of physical and psychological well-being, and the implications for safeguarding the nation's integrity.

A panel of mental health and personnel security experts provided insights that not only underscored the importance of addressing mental health within security blueprints, but also heralded the meticulous understanding of adjudications in the continuous evolution of the complex world.

Since its inception in 1949, the month of May has been recognized as Mental Health Awareness Month and has served as the cornerstone for addressing the challenges faced by millions of Americans living with mental health conditions. Throughout the month, national and local media, pop-up shops, film screenings, etc., highlight resources for recovery and address the stigma preventing individuals from being proactive and seeking out the care they need.

The Personnel Security (PS) directorate hosted this webinar in the hopes that attendees retain a thorough understanding of how national security experts and background investigators analyze mental health treatment and make determinations as to who is eligible to receive access to classified information via a security clearance.

Elizabeth Bolin, PS Curriculum Manager for the Center for Development of Security Excellence, began the discussion asking Dr. Rebecca Blood, Installation Director of Psychological Services, Ft. Meade, "how is confidentiality incorporated in mental health treatment for a patient with a clearance?"

"Confidentiality is a boundary that we as mental health professionals must always enforce. Cleared employees may seek out mental health treatment without any disclosure to their command," said Blood. She further explained that there are exceptions that warrant the breach of confidentiality

and reporting to command. Those exceptions can include hospitalizations, issues arising during treatment that impact judgement, substance abuse, as well as repeated rule violations.

The stigma associated with reporting mental health issues can be inadvertently associated with how question #21 (Q21) is worded on the Standard Form 86, Questionnaire for National Security, making issues appear more adverse and/or complex than they are. The question states, “Does the person under investigation have a condition that could impair his/her judgment, reliability, or trustworthiness?” Often, clinicians answer the question in relation to the condition itself and not specifically to the respective patient. Additionally, based on the new criteria, the threshold for reporting and determinations is broad as there is no diagnosis that is considered automatically disqualifying.

However, several policies, such as Executive Order 12968, DOD Instruction 6490.08, and revisions to Q21 in 2008, 2012, and 2017 have resulted in numerous cleared individuals avoiding treatment when needed, in addition to senior leadership not encouraging treatment due to the fear of an employee not fulfilling a particular billet. However, from a security perspective, seeking behavioral or mental health treatment is promoted because it mitigates security concerns, ultimately decreasing the risk of cleared individuals breaching national security.

Dr. Phillip Atkinson, Operational Psychologist for the DOD Insider Threat Management and Analysis Center (DITMAC), stated that there is a lot of room for “misunderstanding and unproven misconceptions” on how insider threat professionals use mental health statistics. “Everyone within DCSA should know that if they need help, then they should absolutely get help,” said Atkinson.

Insider threat programs are designed to evaluate concerning behaviors and determine if an individual poses a risk to DOD personnel or national security. The programs are comprised of background investigators, human resource personnel and mental health professionals that apply expert analysis of ongoing cases. Furthermore, the highest standards of respect for confidentiality and the safeguarding of mental health information are always followed.

Every cleared employee goes through the adjudication process. During this process, adjudicators analyze and consult with several insider threat professionals and mental health experts to determine whether a potential employee is granted, denied, or even revoked for a security clearance. Adjudicators use the Security Executive Agent Directive-4 Whole-Person Concept to make their final determinations. The concept uses the adjudicative guidelines in conjunction with a full scope review of a candidate’s psychological patterns and history.

Even beyond psychological patterns, the Behavioral Science Branch (BSB) of Adjudication and Vetting Services (AVS), applies due process to resolve complex medical records. “We wanted to have a specialized focus on cases that are complex, specifically those involving alcohol and substance abuse,” said Dr. Elisabeth Jean-Jacques, Senior Staff Psychologist, AVS. The BSB collaborates alongside with a team of adjudicators to determine the best course of action for candidate and/or employee eligibility. “I want the DCSA workforce to know that we analyze the full person,” said Jean-Jacques. “We are committed to giving everyone a fair chance.”

“Losing or failing to gain clearance eligibility for psychological conditions, in and of themselves, is very rare,” said Dr. Michael Priester, Chief Behavioral Scientist for AVS. Between 2012 – 2023, less than 1% lost or did not gain clearance eligibility. Even in combination with other factors, it is rare to lose clearance eligibility.

“Most of the individuals who lost or did not gain eligibility, had as many as six violations,” said Priester. “Showing poor candor can raise much more of a security concern, so being honest on the SF86 can increase your chances of retaining or gaining eligibility.”

The webinar served as a catalyst for demonstrating the vulnerabilities posed by untreated mental health conditions. Weaving the threads of adjudication and vetting services in conjunction with discussions on mental health, creates an inclusive environment that encourages the act of seeking out resources and support.

“It is abundantly clear that the collective security of the nation is connected to the well-being of our minds,” said Priester. “Fortifying our resilience and promise as Gatekeepers, reaffirms our commitment to the nation.”

“ONE PS:” Unified mission strengthens personnel security

By Lena Burns
Personnel Security

On any given day, you'll find a background investigator somewhere across the country, diving deep into the family life, work experience, education, and connections of a person applying to work for the federal government.

Somewhere else another is adjudicating a potential security concern discovered during the vetting process.

And at the very same time, there is yet another individual who is investigating an established federal employee after receiving an alert due to an alleged security violation.

This is what the gatekeepers who make up the Personnel Security Directorate do as part of the Defense Counterintelligence and Security Agency.

They keep Americans safe from those who seek government work with ulterior motives in mind – to cause harm or steal government secrets by gaining access to protected information.

At face value it might seem that each functional area – Background Investigations (BI) and Adjudication and Vetting Services (AVS) are separate entities on their own, with a very specific list of checks and balances, to ensure national security.

But the reality is these functional areas are tightly and intricately woven together. What one area does, directly affects the other, and just as a well-oiled machine relies on the well-being and functionality of each part, the functional areas in Personnel Security operate in a similar fashion.

For example, when AVS receives an investigation request, its personnel security specialists review for issues and completeness to aid in the background investigation process. The investigation is then scheduled and released to BI for action. Once complete, BI provides a product for the AVS Adjudicators to review and make a final eligibility determination.

But this connection goes beyond the operational standpoint, as it also applies to unifying the workforce.

Assistant Director for Personnel Security Dr. Mark Livingston believes that what PS does every day starts with the people.

“Our mantra here at Personnel Security is mission first, people always. Putting into perspective, of course that mission is paramount, but we can't get the job done without people and that is the foundational springboard for our One PS effort,” he said.

When Dr. Livingston came on board in June 2022, the directorate was divided into three parts: Background Investigations (BI), Consolidated Adjudications Services (CAS), and Vetting Risk Operations (VRO).

Each functional area was working within their silos, concentrating on specific responsibilities — investigating, adjudicating, or managing alerts from continuous vetting.

But as the focus on the big picture of the mission sharpened, it became clear that the directorate needed to unite under the concept of ONE PS. With that in mind, Dr. Livingston directed the merger of CAS and VRO to enhance mission success. The purpose of the merger was threefold; to better use limited personnel and resources, better align DCSA functions to Trusted Workforce 2.0, and to enable effective protections from threats to the United States.

He considered the efficiency of all facets of the security operations, customer satisfaction, employee professional development, and greater mission success. CAS and VRO combined are now renamed Adjudication and Vetting Services, otherwise known as AVS.

Dr. Livingston believes this move is a gamechanger.

"I think the merger is four key areas for me," he said. "I think the people benefit because of the importance we place on people. I think for the organization, resiliency is there because it makes the organization slack tighter so that we get better results, then I think about the advanced capabilities going forward in the future and then the end state is a much better organization built for the future."

With the people of PS at the forefront of this unity of effort, steps are also being taken to ensure that the workforce in each functional area know and understand what the other is doing. That connection is supported in various ways, bringing the functional areas together will reduce the workload and result in efficiencies.

Also getting together in a social setting is another way for the workforce to not only connect, but bond as well, which is having a positive effect on morale and motivation. Last year's summer event and winter holiday party both garnered a record number of attendees, with many people saying they appreciate the opportunity to interact with senior leadership in a relaxed environment. They also appreciated the opportunity to meet other colleagues for the first time.

Transparency is also a priority in PS. When senior leaders gather for an off-site, the workforce gets an update on what was accomplished. Sometimes that's in the form of a personalized video message from Dr. Livingston or shared through PS leadership and supervisors.

Communication, working, and socializing together are all key components in unifying the workforce.

Background Investigator Tekia Winder, who has been with the agency for 16 years, participated in an effort that helped reduce a backlog of cases by more than 60,000. She said getting the opportunity to work with others outside her area of expertise was a great experience and gave her valuable insight into what her colleagues in other areas do every day.

"It's satisfying to know we all play an important part in national security. The opportunity to see the skills we all bring to the table also emphasize the fact that we are all in this together," Winder said.



DCSA Director David Cattler stands with Assistant Director for Personnel Security Dr. Mark Livingston and the rest of the Personnel Security team at Fort Meade, Md.

Regional summit strengthens integration of missions, outlines way forward

The Defense Counterintelligence and Security Agency's Eastern/Mid-Atlantic Regional Summit, held in Clearwater, Fla., from May 14-16, brought together Eastern and Mid-Atlantic region leaders to strengthen integration and discuss the future of the agency.

The conference provided a venue for conversation, feedback, and an opportunity to strengthen the integration of service provisions. This year, an emphasis was placed on aligning efforts under DCSA Director David Cattler's vision of ensuring DCSA is known as the premiere provider of integrated security services.

Over three days, the summit served as a platform for coordination and strategic dialogue, reflecting the collective commitment to achieving full mission performance and preparing the agency for future challenges.

"Conferences like this are really important, not just for the cross talk, information sharing and integration piece, but also, the camaraderie. There's a lot to be said interacting and talking to people in a setting like this," said Daniel Lecce, deputy director of DCSA. "The true strength of this agency is integration—we can produce an operational threat picture that nobody else can produce."

Stressed by multiple senior leaders, the importance of unifying mission areas to enhance overall agency performance is critical. This included discussions on personnel security, where the emphasis was on safeguarding classified information, process and application of security practices and reviews, and ensuring the workforce is well-trained to mitigate threats.

Leaders also underscored the critical role of industrial security in protecting classified technologies and facilities, while also integrating counterintelligence efforts to detect and deter espionage activities.

Human resource management and diversity, equity, and inclusion were highlighted as vital to attracting and retaining top talent, fostering an inclusive workforce, and enhancing employee engagement. These discussions aimed at ensuring that DCSA remains competitive and resilient in a dynamic job market.

Mission Support and Chief Strategy Office sessions focused on aligning strategic objectives with operational capabilities. This involved integrating new technologies and innovative practices to streamline operations, ensuring the agency remains agile and effective in mission accomplishment.

Cybersecurity and Authorizing Officials provided information addressing evolving ability, changes, and the need for robust measures to protect systems and information. Continuous monitoring and advanced cyber defense strategies were emphasized as essential to maintaining agency resilience.

The Employee Council and the Center for Development of Security Excellence (CDSE) stressed the importance of professional growth, continuous learning, and the evolution of training opportunities across the workforce. Initiatives aimed at providing ongoing training and development opportunities were discussed, reinforcing leadership commitment to nurturing a skilled and capable workforce.

The Office of Communications and Congressional Affairs underscored the need for a consistent and clear communication strategy. Engagements with Congress and other stakeholders was highlighted as crucial to building strong relationships and ensuring mission support.

Overall, the conference successfully fostered a sense of unity and strategic focus among DCSA leaders and managers. The event underscored the collective commitment to realizing the director's vision of DCSA as the premier integrated security services provider and preferred security partner.

CI chief of staff gains valuable experience at White House detail

By Beth Alber

Office of Communications and Congressional Affairs

Growing up in Southern California, Barbara Holston didn't realize she was different. The daughter of Taiwanese immigrants, she grew up in Monterey Park, California, ensconced in a city whose population was more than 60% Asian American. While she spoke English in school, Mandarin was the primary language at home. Her family celebrated traditional Chinese holidays, such as Lunar New Year. When Holston's grandparents were alive, the family would often travel to Taiwan for the holidays, but the last time she made that trip was over 30 years ago.

"My parents came to this country 50 years ago seeking the American dream. When they came to this country, my parents left my older brother with my maternal grandparents for five years while my parents went to graduate school and were able to solidify a job. They instilled in me my hard work ethic, to be proud of our history, and to retain the culture, such as sending me to Mandarin school during summer breaks, and it is embedded in me to this day the importance of honoring my history," the chief of staff of the Counterintelligence (CI) and Insider Threat directorate said.

It wasn't until Holston got married in her early 20's, became a military wife and left Southern California, that she realized she was a minority in this country – in more ways than one. As a military spouse, she found it hard to find consistent employment, despite having a degree and experience.



Barbara Holston (left), chief of staff of the Counterintelligence and Insider Threat directorate, stands with Erika Moritsugu (center), Deputy Assistant to the President and Senior AA and NHPI Liaison to the White House, and Krystal Ka'ai, Executive Director of the White House Initiative on Asian American, Native Hawaiian, and Pacific Islander, and the President's Advisory Commission on Asian American, Native Hawaiian, and Pacific Islanders, after the DCSA observance for Asian American Native Hawaiian Pacific Islander Heritage Month on May 21. (DOD photo by Christopher P. Gillis)

"Our first duty station was in Missouri and I quickly realized that nobody looked like me. I left a lucrative career in Southern California as a senior staff accountant and quickly found myself unemployable as a military spouse," she said. "I was actually not desired, even though I had the credentials and experience."

While Holston had the opportunity to move around with her husband, there were times she struggled to progress her career. During these times, she'd volunteer on the military base supporting military families. Community and culture have always been important to Holston.

When the pandemic hit and the Asian American community was the victim of hate crimes, Holston looked for ways to support her community. She volunteered time in support of Asian American, Native Hawaiian, and Pacific Islander (AA and NHPI) events, and worked on leadership conferences with the Federal Asian Pacific American Council (FAPAC), a nonprofit organization representing the federal civilian and military AA and NHPI community. Through her support of these events, she was specifically requested to run as part of a special election for the FAPAC National Board of Directors. During a FAPAC event in 2022, Holston met Erika Moritsugu, Deputy Assistant to the President and Senior AA and NHPI Liaison to The White House. Moritsugu was the keynote speaker at the event, and Holston was seated beside a detailee from Moritsugu's office.

"The detailee and I hit it off when talking about our jobs and backgrounds, and she asked if I would meet for coffee," Holston said. "We met two months later and she asked if I would consider coming to The White House, because I had the personality and skills that would work well for Erika's office."

Holston had just been selected as the CI chief of staff, and while she wasn't ready to take that leap, she didn't want to disregard the amazing opportunity. Holston joined CI in 2019, as a senior program analyst; transitioning from a career budget analyst. "I had a history of taking care of my programs, ensuring priorities were considered at the financial level, which allowed me to showcase to senior leadership that I cared about their outcome and success," Holston said.

"I might not be a trained CI person, but I can get them to a place where their priorities are considered and their concerns are heard," she continued.

However, the opportunity to serve her community in a White House detail was always on her mind. After a couple of months, she approached the detailee and asked to meet Moritsugu. After chatting over Zoom and exchanging emails, Holston quickly became the first Department of Defense detailee within the White House Chief of Staff Office supporting the AA and NHPI office that was created in 2021 by the Biden-Harris Administration.

Since November 2023, Holston assisted in drafting Presidential statements, to include a statement marking the one year anniversary of the mass shootings in Monterey Park and the 80th anniversary of the Repeal of the Chinese Exclusion Act; she helped develop social media posts, to include marking the 35th anniversary of the Cleveland Elementary School shooting in Stockton, Calif., where Southeast Asian children were victims of a hate crime; and she assisted in creating a celebration of Lunar New Year and AA and NHPI Heritage Month at the Vice President's residence. She also provided opening remarks at the Pentagon's AA and NHPI Heritage Month where she highlighted the importance of diversity in all echelons of leadership, as well as the importance of empowering the next generation. She traveled with the White House and the White House Initiative on AA and NHPI for their regional economic summits and their community engagements with the President's Advisory Commission on AA and NHPI. "These statements and events were intentional about being inclusive. I am proud of being there for critical moments to bring joy and positivity," she said.

Additionally, Holston met survivors of Japanese-American internment camps and Southeast Asians who fought in the Vietnam War and quickly realized that the history books don't always capture the totality of their stories. "It's important to make sure the stories are not lost," Holston said. "I had not heard many of these stories and that has changed me as a leader and as a person. It gave me an appreciation for those who have paved the way for someone like me."

Finally, she is proud that she has been mentored by senior leaders within the White House and also provided mentorship to White House interns, staff and colleagues. "Coming up in the federal government, I rarely saw somebody who looked like me sitting at the table," she said. "It was important to me to show the next generation what is possible."

"Knowing our history gives us power and purpose, and diversity and representation matters," Holston continued.

"Policies and decisions are better cultivated when you have a diverse workforce. I am proud of my mentorship, because when you see others that look like you, you know what's possible."

NHL team honors DCSA security manager as hometown hero

Philadelphia Flyers cite military service, current DCSA position

PHILADELPHIA – Jessika Szatny was taken by surprise when the Jumbotron kinetically displayed her wedding day picture via 6,601 square feet of 4K LED video technology above the Philadelphia Flyers hockey rink.

She was among tens of thousands of hockey fans viewing pictures of her husband, Defense Counterintelligence and Security Agency (DCSA) Eastern Regional Security Manager Reggie Szatny, while he was deployed as an active-duty U.S. Army soldier with the 1st Cavalry Division's Iron Horse Brigade in support of Operation Enduring Freedom and Operation Iraqi Freedom.

What's more, the fans attending the Philadelphia Flyers versus Buffalo Sabres hockey game in person and via national broadcast from the Wells Fargo Center listened with the Szatnys as an announcer cited Reggie's military accomplishments and current DCSA position while honoring him as a Philadelphia Flyers Hometown Hero on Nov. 1, 2023.

The picture of the couple on their wedding day with Reggie in military dress uniform was a photo he provided to the Flyers in response to the Hometown Hero surprise Jessika set in motion when nominating her husband for the program unbeknownst to him.

"I felt so proud of Reggie's dedication and service to his country put out there on the Jumbotron while his entire service career and awards were announced," she said. "It was really exciting to be there and to be a part of that with him. I was just extremely proud of him and everything that he has done."

As season ticket holders, the couple would see a Hometown Hero – usually a National Guard or military reserve veteran – honored during every game. Jessika began thinking about nominating her husband who was medically retired in 2016 after fourteen-and-a-half years of active-duty service.

"I started thinking about all the things that he has done – the awards he earned, everything in his career – and wanted to nominate him."

One day, Jessika furtively submitted the nomination via the Flyers Hometown Hero online nomination page. A year-and-a-half later, she decided to renominate Reggie for the program and was about to do so, but it wasn't necessary.

"I received a phone call out of the blue from the Flyers with the news that Reggie was selected to be the next Hometown Hero," said Jessika. "I was super, super surprised since my nomination was submitted so long ago and at the same time, very excited because I wanted to see him recognized in front of many people for everything that he's done."

Jessika kept the good news under wraps, but the Flyers eventually contacted Reggie, which included a request for pictures.

"When I saw an e-mail from the Flyers about my selection due to the Jessika's nomination, it made me so proud that she did that," said Reggie. "The event was also amazing for my children. It was the first important thing for them regarding my service since they were never able to experience too much when I was in the military. It was a fantastic culmination of my whole career."

Reggie, Jessika and their children – daughters Mackenzie, Riley and son, Zyler – gathered together during the ceremony as the moderator announced their names, including the oldest son, Reggie III, who was not in attendance. Reggie's bio was highlighted for the audience as they became acquainted with the Flyers Hometown Hero, his family, and service throughout his military career.

"Sergeant First Class Reggie Szatny is originally from the Fishtown/Kensington section of Philadelphia and grew up in Pine Hill, N.J. He joined the U.S. Army at the age of 31 to serve his country after the events of 9/11 in May 2002 as an Army Communications specialist, first stationed in Landstuhl, Germany," said the announcer, who cited Szatny's awards, which included two Meritorious Service Medals, four Army Commendation Medals, an Army Achievement Medal, a Meritorious Unit Commendation, a National Defense Service Medal, an Iraq Campaign Medal with two Campaign Stars, and the Global War on Terrorism Service Medal.

At that point, the Flyers' ambassador of hockey Bob Kelly, a member of the famous 'Broad Street Bullies' who helped lead the Flyers to their two consecutive Stanley Cup championships in 1974 and 1975, presented a custom Flyers military-style jersey to Reggie.

As the family walked back to their seats to watch the remainder of the game, Reggie heard social media notification pings from his cell phone, one after another.

"I have a very unique name that people remember," he explained in reference to people he did not see or communicate with since high school who were watching the game and looked him up to touch base and say congratulations.

"He was getting messages saying – 'Hey, I saw you. Oh my gosh, congratulations, well deserved' – from so many people," said Jessika. "Some of my co-workers were like, 'I saw your husband getting recognized last night and that was so awesome. Please tell him, 'Thank you for his service' for us.'"

The Flyers Hometown Hero program was developed to recognize local (Philadelphia metro area) men and women who are serving or have served in the past 10 years with one of the nation's five armed forces.



NHL Team Honors

Reggie Szatny – holding the military-style hockey jersey – is honored as a Hometown Hero at a Philadelphia Flyers hockey game. Fans attending the game in person and via national broadcast listened to his military accomplishments and current Defense Counterintelligence and Security Agency position as Eastern Regional Security manager announced at the Nov. 1, 2023 ceremony.

Standing with Szatny are his wife, Jessika and children – daughters Mackenzie, Riley and son, Zylar.

Pictured on the left is Bob Kelly, a member of the famous 'Broad Street Bullies' who helped lead the Flyers to their two consecutive Stanley Cup championships in 1974 and 1975, who just presented the custom Flyers jersey to Szatny.



Defense Counterintelligence and Security Agency

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil

571-305-6562

www.DCSA.mil