Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper

Volume 2, Issue 3

CI and Insider Threat reorganizes and refocuses on key missions

IN THIS ISSUE

IN THIS ISSUE

Vol 2 | ISSUE 3

DCSA Gatekeeper

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

From the Director

Many readers of the Gatekeeper have heard me speak at various industry fora to share my vision for DCSA's future and related mission performance updates. If so, you have heard me speak of the changing threat landscape as decades of focus on counterterrorism have yielded to the more concerning recognition of great power competition's potential consequences. The innovation resident in our industrial base and our ability to protect it—through our industrial security team's partnership with cleared industry—has never been more critical to our nation's future than it is today.

This issue of the Gatekeeper focuses on one component of that partnership: the work of DCSA's Counterintelligence and Insider Threat Directorate (CI). Besides providing our Industrial Security and Personnel Security teams with a detailed threat picture to inform their risk analysis, CI assists industry directly by identifying threats to our critical information, technology, and personnel. They paint a threat picture that enables industry and others to understand the nature of attacks on the cleared industrial base and also supports intelligence operations and criminal prosecutions that protect our national security.

This issue also provides two articles that demonstrate DCSA's commitment to supporting our customers and stakeholders with next-generation IT capabilities. The article on the "NBIS Playground" demonstrates how our cutting-edge IT development process can deliver sophisticated technologies faster by allowing users to test new features and identify adjustments earlier in the process during the design and engineering phases. Ongoing collaboration between the NBIS technical team and DCSA's Adjudications, Continuous Vetting, and Background Investigation teams will ultimately lead to a better product for all users much sooner than would have been possible using traditional acquisition processes.

Another example are the improvements being made to the National Industrial Security System or NISS found in the Personnel Security Investigations for Industry (PSI-I) annual projections survey. When NISS became the system of record for facility clearance information in 2019, it suffered from myriad user-experience challenges. Since then, DCSA has worked diligently to enhance the overall user experience and streamline processes to reduce the burden on industry.

Finally, this issue reports the substance of DCSA's first fireside chat with Dr. Stacey Dixon, Principal Deputy Director of National Intelligence. Dr. Dixon's visit highlighted the importance of DCSA's role in transforming the U.S. Government's personnel vetting landscape.

Thank you for your dedicated work as we continue to improve our performance as America's Gatekeepers.

William K. Lietzau
Director,
Defense Counterintelligence
and Security Agency

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.

Special Agent Andrew J. Lochli is the Assistant Director, Counterintelligence and Insider Threat Directorate

In this capacity, he directs the agency's efforts to identify, assess, disrupt, and mitigate threats to cleared industry, the trusted workforce, the Department of Defense and DCSA through the application of counterintelligence (CI), cyber, and enterprise insider threat management activities.

Prior to joining DCSA, Special Agent Lochli served as an Executive Assistant Director with the Naval Criminal Investigative Service (NCIS), serving as Director of the Office of Commercial and Economic Analysis — Navy (OCEA-N), Naval Intelligence Activity. At OCEA-N, he enabled the defense of Department of the Navy equities by identifying and characterizing economic threats through analysis and information sharing, while developing actionable mitigation plans in support of the National Defense Strategy.

Prior to leading OCEA-N, Special Agent Lochli served as the Assistant Director, NCIS Cyber Directorate where he provided direction, oversight, and coordination of criminal and CI investigations and operations in the cyber domain.

His former senior leadership positions include serving as the Deputy Assistant Director (DAD) for Criminal Investigations and Operations; Executive Assistant to the Deputy Director; DAD for CI Investigations; and Division Chief for Criminal Operations and Transnational Crimes.

Special Agent Lochli's prior supervisory positions include serving as Assistant Special Agent-in-Charge for General Crimes, NCIS Northwest Field Office; and ASAC for Counterintelligence, NCIS Hawaii Field Office. He served previously as the Supervisory Special Agent (SSA) of the NCIS Resident Agency, Kaneohe Bay, Hawaii; SSA Office of Special Projects, Washington, DC; and SSA, NCISHQ Counterintelligence Directorate.

Special Agent Lochli joined NCIS in 1999 with initial assignments in Bremerton, Washington and Marianas, Guam. In these assignments, he worked across NCIS general crimes and counterintelligence mission areas. Special Agent Lochli is a credentialed Certified Fraud Examiner (CFE).

QUESTIONS AND ANSWERS

We have your biography, but what would you like readers to know about you and the CI and Insider Threat Directorate?

The vision of the Counterintelligence and Insider Threat Directorate vision is to out PACE counterintelligence (CI), cyber, and insider threats (InT) through production, analysis, collection, and engagement.

The Directorate produces a variety of classified and unclassified products for its customers—industry, the Intelligence Community (IC), other government agencies (OGA), and other DCSA directorates. These products provide critical intelligence on foreign intelligence entity (FIE) emerging and future patterns, trends, and threats to cleared industry. We distribute products such as the Annual Trends Report to Industry, Intelligence Information Reports and finished intelligence to keep the IC, government and industry partners abreast of FIE targeting cleared industry, and Cyber bulletins and reports to identify threats and vulnerabilities. The Directorate also produces referrals to provide to OGA partners. These referrals are based on the collection and analysis of information received from industry, and provide OGA's operational or investigative opportunities to disrupt, neutralize and exploit the FIE threat.

Our CI and Cyber divisions analyze information reported by cleared industry to identify the FIE threat, their methods of operation, method of contact, and affiliations, and is used to produce the aforementioned products to its customers and stakeholders. In addition to the CI-centric products, the Department of Defense (DoD) Insider Threat Management & Analysis Center (DITMAC) and the Operations Analysis Group (OAG) analyze InT reports submitted by the DoD and cleared industry in order to provide recommendations for mitigation.

We have various methods of collecting information regarding suspicious FIE and InT activity from cleared industry. Industry provides suspicious contact reports directly to DCSA CI Special Agents, which is then analyzed by CI and Cyber analysts. The Joint Cyber Intelligence Tool Suite (JCITS) maps cleared contractor public infrastructure and fuses those maps with known cyber-attack patterns of FIE. Using the information gathered from JCITS, Cyber analysts provide assessments to cleared contractors. With regards to insider threat, DITMAC and the OAG rely on the DoD InT component hubs and cleared industry to report individuals whose behavior meets the criteria of one or more reporting thresholds.

Our success lies within its engagements and cooperation with other DCSA elements, the IC, Law Enforcement (LE), Cyber, National CI Task Force (NCITF), and cleared industry. Each of these groups is vital in helping TD support the DCSA mission. Close relationships with other DCSA directorates ensures that we can provide the necessary CI and InT support required to secure the trusted workforce. Engagements with the IC, LE, Cyber, and NCITF enable us to disrupt and mitigate threats to industry.

What led you to this position at DCSA?

I have 22 plus years at NCIS with a diversity of assignments in general crimes and counterintelligence in both the field and at headquarters. What led me here is timing, opportunity and it was a big challenge. I had worked with the Defense Security Service (DSS) years ago as a junior agent doing background investigations in Guam. I had also worked with DSS when I was in charge of CI Investigations for NCIS as well as when I was the Assistant Director for Cyber. I saw this position as a tremendous opportunity and a tremendous challenge. The traditional CI, cyber and insider threat environments continue to evolve and we face an ever-changing landscape of our adversaries employing non-traditional techniques. I saw DCSA as an opportunity to bring my CI experience as an 1811 Special Agent, challenge myself to do more and contribute to the continued success, growth and impact of DCSA, NCIS and our colleagues and partners.

How does the directorate support the agency's mission?

The directorate supports the agency's mission of securing the trustworthiness of the U.S. Government's workforce, the integrity of its cleared contractor support and the uncompromised nature of its technologies, services and supply chains primarily through industry engagement and CI support.

Directorate personnel conduct CI functional services within cleared industry through CI awareness briefings, travel pre- and de-briefs, and the collection of FIE threat information. We provide timely and informative threat products based on collection and analysis, and engage with cleared industry by hosting unclassified monthly CI webinars and hosting cleared industry representatives to facilitate information sharing. All of these activities assist the agency in protecting technologies, services, supply chains, and personnel.

Additionally, to ensure the trustworthiness of the workforce and the integrity of cleared contractor support, DITMAC and the OAG identify and develop responses to significant vulnerabilities, unmitigated threats, and policy gaps within the national industrial base and the DCSA Personnel Security mission.

You recently took a trip to visit field sites. What did you learn?

I visited the Western Region soon after taking the job. As an NCIS agent, we typically move to different locations and offices every few years. While we always strive for consistency, no office is the same. Different locations present different circumstances such as varying mission priorities, staffing and costs of living.

Our people are our most important resource and the most important thing you gain from going out to the field is listening and hearing their perspective. I have found that you need to go out to the field to gain the pulse and perspective of what day to day operations are like in the area. For instance, where their successes are, where they need help, what challenges they encounter and what goes in executing the mission at a high level. This may be IT challenges, facility challenges, commutes, cost of living, retention, etc. You can't get this from a PowerPoint brief or metrics; they just don't capture what you get from that in-person perspective. In addition to listening, I also appreciate being able to share perspectives/priorities from headquarters, where we are going with the Directorate and ensure that everyone can contribute and have a voice as the Directorate moves forward. This just can't be captured in a metric.

What stood out the most to me in the west was the people. As the "new guy", I was welcomed with open arms by the team. I know everyone is busy, but personnel from all the disciplines, CI, Industrial Security and BI all took time to meet with us. I met folks from throughout San Diego, personnel drove down from Los Angeles and I had VTC's with Fremont, Pasadena, Albuquerque, Phoenix and Hawaii. The most impressive aspect was the integration of personnel between CI, BI and Industrial Security. As an agency that has brought together many different organizations over the past few years, the integration, collaboration and partnerships across the disciplines was extremely impressive.

What are the biggest initiatives on going in the Directorate?

In short, setting mission priorities. We do a lot of great work across CI, Cyber and Insider Threat. We have a growing demand signal within the agency, across our government agency counterparts and in industry, but have limited resources. We need to grow personnel, particularly in the field (CISAs, Analysts and Cyber personnel), to meet the continuous threats and the growing demand. We also need to educate the agency, our counterparts and industry on the uniqueness of DCSA and what we contribute to the fight. DCSA has unique placement and access and leveraging DCSA will complement and enhance a more holistic approach and greater impact to National Security.

What do you see as the biggest counterintelligence threats facing the agency?

Modernization of adversarial techniques and keeping pace with technology. Our adversaries don't play by the rules. We cannot approach today's adversaries the same way we did 10, 20, 30 years ago. We need to modernize, adapt and be agile enough to pivot to new and emerging threats. We also need to recognize new battlespaces such as cyber, insider

threats and legal avenues that adversaries use to gain an advantage. We have to keep pace with evolving technology so we can identify and eventually predict emerging threats (through accelerated capabilities and tools). Countering and mitigating threats today may now come down to minutes and hours vs days and weeks.

The DITMAC was recently realigned under the Directorate. Do you see this as a natural fit for DITMAC?

It makes sense as threats, whether CI, Cyber or Insider Threat cut across the agency's mission. Insider Threat was historically CI focused and the mission has evolved and modernized to include everything from spies, to criminal threats, to personal conduct that could pose risk. Having these focus areas together, interconnected and overlapping, will make our unity of effort and results to identify and mitigate threats even stronger.

What are the biggest challenges facing the Directorate?

Additional people and resources to execute the mission.

We need to enhance education, awareness and information sharing across the agency, government and industry. DCSA's unique placement and access to industry make us a key component and critical force-multiplier to leverage, synchronize and complement whole of government efforts in protecting our workforce, industry and our national security. By enhancing our technology and capabilities, we can accelerate analysis and info sharing through better tools.

CI and Insider Threat reorganizes and refocuses on key missions

Shortly after Andrew Lochli arrived at DCSA to take the helm of Counterintelligence, the office was reorganized to encompass the DOD Insider Threat Management and Analysis Center (DITMAC) and Operations Analysis Group (OAG), and renamed the Counterintelligence and Insider Threat Directorate. The goal of the reorganization was to provide unity of effort across similar disciplines and provide a more comprehensive, holistic threat picture to industry and government stakeholders. With the reorganization, the Counterintelligence (CI) portion of the mission was also undergoing an analysis of its work products with an eye on refocusing its efforts on the depth and breadth of CI functional services, collection, and analysis and production across the National Industrial Security Program (NISP), Trusted Workforce, and DCSA Enterprise.

Allison Carpenter, Deputy Assistant Director, Office of Counterintelligence, explained. "Like everyone else, we faced significant challenges during the pandemic. CI is largely a human-based discipline," she said. "The CI mission and professionals thrive when we meet face-to-face, share classified threat information, and discuss mitigation strategies. Despite the hurdles of working remotely, we continuously engaged cleared industry through telephone and email, and still enabled the identification and disruption of adversaries targeting classified technology, sensitive information, and cleared personnel."

Carpenter noted that in addition to the challenges inherent in remote work, the CI workforce changed drastically over the past two years. "We said farewell to CI professionals who have served the Department for over three and half decades," she said. "We also welcomed our first developmental agents and analysts to grow our future CI workforce from within, developing diversity through age, gender, ethnicity, and background/experience."

As COVID restrictions ease and employees return to in-person engagements, she noted that employees hired during the pandemic have had limited opportunities to apply their CI prowess on the ground at facilities. "We know transitioning the workforce back to boots on ground engagements means re-learning how to execute the daily mission," she said.

In short, the turmoil of the past two years led CI to establish new priorities and focus on the following core CI activities:

Engage and Collect. CI is focused on quality engagements with cleared industry through CI threat briefings, CI support to Security Reviews, and Advise and Assist visits. It also emphasizes building and re-establishing relationships with industry post-pandemic.

Refocus Analytic Efforts and Priorities. CI prioritized publishing the trends report (classified and unclassified), and delivering threat products (threat advisories, warnings, and reports) that assist in articulating threat information directed at the cleared industrial base to industry stakeholders, the Intelligence Community, and U.S. government partners. This summer, CI reestablished Secure Video Teleconferences with cleared industry through the CI Partnership with Industry program to reach the maximum number of facilities and personnel.

Integration and Information Sharing. CI found opportunities to share CI information with stakeholders. This includes establishing and implementing initiatives to integrate CI functional services within the DCSA enterprise.

"These efforts allow CI to get back to basics with engagement and analysis," said Carpenter. "Engagement connects us to our primary customers, builds the picture of the threat landscape, and facilitates our ability to promote information sharing and collaborate with our partners. As DCSA expands, so must our support to other DCSA mission areas and enabling elements."

Implementing these CI mission areas are the two main divisions within CI -- Operations and Analysis. The Operations division is the link between the Counterintelligence Special Agents (CISAs) spread across

the country and the headquarters. CISAs execute the CI mission by interacting directly with cleared industry through threat briefings, providing feedback and input to CI analysts and serving as liaisons with other government agencies.

"CISAs build strong relationships with industry, other government partners, and with DCSA industrial security professionals to ensure timely, accurate information is shared and actioned," Carpenter said. "Their knowledge of facilities, technology, and personnel directly contributes to the deterrence, detection, and disruption of foreign intelligence entities."

Another key mechanism to share threat information with industry is through the CI Partnership with Industry Program which is a collaborative program designed to promote information sharing of CI concerns. The CI Academic Outreach program not only facilitates collaboration among cleared universities in the NISP, it also strives to sensitize them to the threat for foreign intelligence entities. Academia plays a key role in technology research and development pivotal to the United States maintaining the competitive advantage. Unfortunately, foreign adversaries prey on the collaborative environment, cutting-edge work, and diversity of thought within the academic sector.

In addition to working with cleared industry, CI is working to establish collaborative relationships with U.S. Government partners through its Liaison branch. By deploying a cadre of CI Liaisons to the Federal Law Enforcement and Intelligence communities, CI seeks to foster better interagency cooperation as well as potential engagement and training opportunities to the benefit of the larger community.

DCSA CI and Cyber partner with 16 agencies and multiple task forces to enhance communication of threat information and drive investigative and operational activities. Liaison Officers are co-located with the National CI Task Force, National Cyber Investigative Task Force, Export Enforcement Coordination Center, FBI, Naval Criminal Investigative Service, Air Force Office of Special investigations, Army Criminal Investigation Command, Defense Intelligence Agency Supply Chain Risk Management-Threat Analysis Center, National Security Agency, Department of Defense Cyber Crime, and others. These relationships have led to identifying and addressing potential threats and vulnerabilities within cleared industry, through synchronized engagement, mitigation, and disruption efforts.

While the Operations division tends to be the outward face of CI, the Analysis division provides the complex analyses to detect and deter foreign intelligence enterprise attempts to obtain classified and sensitive information and technology. The cadre of analysts in the division gather, synthesize and attempt to fuse reporting from industry with open-source and classified intelligence to form an analytically sound intelligence assessment for industry, DCSA personnel and the larger Intelligence Community.

"As foreign intelligence entities continue to become more prevalent, aggressive, and adaptive, DCSA must be able to communicate the emerging trends and patterns quickly, feeding the need for information and understanding of the threat landscape," Carpenter said.

The Annual Trends Analysis Report has long been the flagship analytic product for CI and was last published in 2020 due to challenges with reporting and analysis during COVID. The Trends report details cleared industry's reporting of potential foreign intelligence entity attempts to illicitly acquire U.S. technologies resident in cleared industry, and identifies the most coveted technology categories as well as the geographic areas most prolific in their efforts to illegally acquire the technologies. The Fiscal Year 2021 classified and unclassified Trends will be published in 2022, with hard copies of the classified Trends reaching stakeholders in the summer 2022.

In addition to the Trends document, the division produces a wide array of threat assessments, reports and referrals in support of the facility clearance and Foreign Ownership, Control or Influence (FOCI) processes.

"Energized by the focus on great power of competition, DCSA CI continues to build partnerships, seek to identify and counter foreign intelligence threats, and share information that will impact risk-based decisions within industry and government," said Carpenter. "The pandemic may have changed how CI executed business on a daily basis, but it did not waiver the commitment to protect and defend critical and sensitive technologies, facilities, and personnel.

"DCSA CI is sharply focused on re-engaging with all partners, driving identification of suspicious contact reports, communicating threats to customers and stakeholders, and growing the mission to meet evolving needs," she concluded.

CI Cyber Mission Center conducts CI activities in cyberspace to identify and neutralize foreign adversary threats

Every day, foreign adversaries attempt to access information resident in the Defense Industrial Base (DIB). When successful, these efforts can compromise critical U.S. programs or technologies and erode our nation's economic, intellectual property, and military competitive advantage. The DCSA Cyber Mission Center (CMC) implements CI activities in cyberspace to identify, assess, exploit, degrade, counter, and neutralize these foreign adversary threats.

The CMC works closely with intra-DCSA elements, DoD Components, U.S. Government departments and agencies, and cleared contractors through the identification, integration, and sharing of threat information to drive risk-based, data-driven decisions and actions. CMC's priority activities include:

- Identifying, assessing, and disrupting threats to cleared industry, cleared personnel, DOD, and DCSA
- Analyzing and anticipating foreign intelligence entities' cyber threat events
- Developing actionable foreign intelligence entities' cyber threat information and warnings for resolveng cyber incidents
- Providing cyber threat education and awareness
- Developing cyber capabilities and processes that illuminate threats, enhance awareness, and enable customer response.

Working with the DCSA Office of Counterintelligence, the Cyber Mission Center has developed a number of cyber programs to assist the National Industrial Base in protecting its information.

DCSA's primary cyber program, the Joint Intelligence Cyber Tool Suite, also known as JCITS, compares known cyber-attack patterns of foreign adversaries against cleared contractor infrastructure to detect vulnerabilities and potentially malicious cyber activities. DCSA shares this information to cleared industry partners to help mitigate cyber threats and vulnerabilities.

JMITT, the JCITS Malware Intelligence Triage Tool, is a platform that ingests emails provided by cleared contractors and conducts a real-time analysis of suspicious attachments to determine whether or not it's malicious. The results of the analysis are then shared with the cleared contractor, DCSA CMC, and the appropriate DCSA Counterintelligence Special Agent to enable mitigation of malicious activities.

Most recently, DCSA's Cyber team developed the Enhanced Cyber Sensor Platform (ECP), which is a congressionally-funded program to perform integrated cybersecurity and counterintelligence to meet three national security focus areas: Threat Intelligence Reporting, Processes for Monitoring Cleared Contract Networks, and Perform Advance Threat Detection Monitoring on commercial networks supporting the Intelligence Community.

The Cyber Mission Center is comprised of 32 cyber employees including CI Special Agents, analysts, computer scientists, program managers, and policy/strategic planners who collaboratively support the aforementioned programs and leverage the resulting data to detect threats, derive intelligence, and generate tailored reports to harden identified targets in support of national security.

In the upcoming year, CMC is prioritizing collaboration and engagement with government and industry partners to increase information, enhance threat awareness, and enable timely customer response for more impactful mitigation of threats to DoD equities.

DCSA leader reminds DOD, industry to prevent inadvertent, unauthorized disclosures; cites recent UD cases

By John Joyce
Office of Communications and Congressional Affairs

Unauthorized disclosures and whistleblowers. What is the difference and why is it important for Americans entrusted with classified and controlled unclassified information (CUI) to understand the difference? In either case — how is national security affected?

DOD Unauthorized Disclosure Program Management Office (UDPMO) Chief Henry Nelson answered the questions from his Defense Counterintelligence and Security Agency (DCSA) office while citing a series of unauthorized disclosure cases, including a case that involves two infamous individuals familiar to the U.S. and international public.

The crimes committed by Julian Assange and Chelsea Manning — responsible for one of the largest incidents of unauthorized disclosure in U.S. history — began when Manning leaked hundreds of thousands of classified documents to Assange for publication on the WikiLeaks website. Classified State Department diplomatic cables, significant action reports filed by U.S. troops and assessments about detainees at the Guantanamo Bay detention camp in addition to visual imagery such as video footage of an airstrike that killed civilians were among Manning's massive uploads to a Wikileaks dropsite.

"We don't know what the repercussions will be but we do know that the impacts of unauthorized disclosure are extremely damaging to national security," said Nelson. "DOD civilians, service members and contractors are privy to some of the most sensitive and closely held information. It is a violation of law and of the oath of office to divulge, in any fashion, non-public DOD information — classified or controlled unclassified — to anyone without the required security clearance, specific need to know and a lawful government purpose. By definition, this would be an unauthorized disclosure. Divulging information in violation of these precepts weakens the department's ability to protect the security of the nation against its adversaries."

"The government takes ... breaches seriously and will use all the resources at our disposal to apprehend and prosecute those who jeopardize the safety of this country and its citizens."

~ Henry Nelson

This unauthorized disclosure of classified information or CUI to an unauthorized recipient can happen in various ways. It can be disclosed intentionally, negligently or inadvertently through leaks, data spills, espionage and improper safeguarding of national security information. When classified information is involved, unauthorized disclosure can be categorized as a type of security incident, characterized as an infraction or violation depending on the seriousness of the incident.

Nelson continued citing examples — including recent and less well known cases — of unauthorized disclosure related to the release of classified information and CUI in the public domain via products such as podcasts, print articles, internet-based articles, books, journals, speeches, television broadcasts, blogs and postings.

In a Maryland case, Mark Unkenholz — a National Security Agency employee who held a Top Secret/SCI clearance with lawful access to classified information

related to national defense closely held by the government (National Defense Information) — was arrested on March 31, 2022 and charged with willful transmission and retention of National Defense Information, according to a news release posted on the Department of Justice (DOJ) website on the same date.

"This mishandling of classified information was intentional and he was charged accordingly," said Nelson, who was the National Geospatial-Intelligence Agency unauthorized disclosure program officer before transferring to DCSA in 2020. "Unkenholz knew exactly what he was doing but was not charged with espionage since he did not send the information to a foreign adversary or release it into the public domain."

According to the indictment, Unkenholz willfully transmitted National Defense Information on 13 occasions between February 2018 and June 2020 to another person who was not entitled to receive it.

If the case involved the release of classified information or CUI to a foreign adversary or publication in the public domain, Nelson and his Unauthorized Disclosure Program Management Office team of case managers and investigators would have been notified.

The UDPMO team — one of several DCSA counter insider threat teams comprising the DOD Insider Threat Management and Analysis Center (DITMAC) — are immediately notified of all incidents involving the release of classified national security information (CNSI) and CUI in the public domain. Notifications to UDPMO include the release or enabled theft of information relating to any defense operation, system or technology determined to be CNSI or CUI. The team is also alerted to incidents of classified information or CUI disclosed to an unauthorized person or persons resulting in an individual's administrative action, referral for criminal or counterintelligence investigation, or the suspension or revocation of a security clearance.

When UDPMO receives a confirmed report of unauthorized disclosure in the public domain, the team submits a crime report to DOJ. Included in the report are findings from a preliminary inquiry conducted by the affected component; a damage and impact assessment; and a media leaks questionnaire for the unauthorized disclosures appearing in the media.

The UDPMO process was exercised in the case of Henry Frese, a former Defense Intelligence Agency employee who pled guilty to the willful transmission of Top Secret National Defense Information to two journalists in 2018 and 2019. As a result of Frese's actions, he was sentenced to 30 months in prison in June 2020.

"Frese violated the trust placed in him by the American people when he disclosed sensitive national security information for personal gain," said Assistant Attorney General for National Security John C. Demers in a DOJ statement. "He alerted our country's adversaries to sensitive national defense information, putting the

DOD Unauthorized Disclosure Program Management Office

The Office of the Undersecretary of Defense for Intelligence and Security realigned the DOD Unauthorized Disclosure Program Management Office (UDPMO) to the former Defense Security Service — now the Defense Counterintelligence and Security Agency (DCSA) — DOD Insider Threat Management and Analysis Center (DITMAC) in 2016.

This transition quickly aligned UDPMO with the DOD insider threat enterprise. Consequently, UDPMO became recognized as a unique mission within DITMAC while its experts worked closely with information security and insider threat advisors. In effect, the UDPMO team at DCSA provides DOD with an enterprise-level management and operational capability to improve identification, reporting, tracking and mitigation of unauthorized disclosures.

DOD officials envisioned that DITMAC's capabilities to identify, assess and mitigate risk from insiders would positively impact the UDPMO mission to oversee and manage unauthorized disclosures that undermine U.S. foreign policy and weaken the ability of the U.S. Government to protect the security of the nation against our adversaries.

nation's security at risk. The government takes these breaches seriously and will use all the resources at our disposal to apprehend and prosecute those who jeopardize the safety of this country and its citizens."

These cases are a reminder to all DOD civilians, contractors and military personnel of their lifelong responsibility to protect and safeguard information. Current and former government, military and contractor personnel with present or prior access to DoD information or facilities must submit materials intended for public release for review and clearance when those materials may contain classified or CUI information to include any work relating to military matters, national security issues or subjects of significant concern to DOD in general.

"This applies while the individual is actively employed with the U.S. government and continues when the individual retires or leaves government service," said Nelson. "Individuals may use the Whistleblower Protection Enhancement Act to report information they reasonably believe provides evidence of a violation of any law, rule, or regulation, gross mismanagement, a gross waste of funds, abuse of authority, or a substantial danger to public health and safety."

DOD Whistleblower Protection allows individuals to report information they reasonably believe provides evidence of a violation of any law, rule, or regulation, gross mismanagement, a gross waste of funds, abuse of authority, or a substantial danger to public health and safety to designated officials via specific channels. Additional information regarding DoD Whistleblower Protection is available on the DoD Inspector General website at www.dodig.mil.

Those making contractor disclosures in response to Federal Acquisition Regulation clause 52.203-13 — Contractor Business Ethics Compliance Program and Disclosure Requirements — can find relevant instructions at www.dodig.mil/Programs/Contractor-Disclosure-Program. The differences between unauthorized disclosure and protected whistleblowing are further clarified at **https://www.cdse.edu/Training/Toolkits/Unauthorized-Disclosure-Toolkit/.**

When unauthorized disclosures and topics of concern are publicized in the media, we release alerts to UDPMO community program managers throughout DOD who are taking proactive steps to prevent unauthorized disclosures.

~ Henry Nelson

The vision became reality and since its realignment to DCSA, the UDPMO team increased its collaboration, outreach and efforts to manage and mitigate unauthorized disclosures of classified national security information and controlled unclassified information.

"We are appropriately placed within DITMAC," said DCSA UDPMO Chief Henry Nelson. "Our outreach and coordination with DOJ on behalf of DOD is increasing significantly and it's key to the program's success. When unauthorized disclosures and topics of concern are publicized in the media, we release alerts to UDPMO community program managers throughout DOD who are taking proactive steps to prevent unauthorized disclosures."

Meanwhile, DOD personnel who suspect or discover an unauthorized disclosure must immediately report it to their security manager. Validated events should be reported through the Insider Threat Program Office or Information Security Office to the UDPMO.

'Subject Matter Expert Office Hours' supports DOD hubs facing insider threat concerns with counsel, collaboration

By John Joyce
Office of Communications and Congressional Affairs

What course of action should a DOD insider threat professional take when facing a challenging scenario involving a government employee, defense contractor or military member exhibiting concerning behavior in the workplace?

As part of the decision process regarding concerning behaviors and potential action, it's important to assess the overall situation and to triage and evaluate the risk of potentially disruptive, harmful, inappropriate, or threatening behaviors towards the DOD.

In larger DOD departments and in those with robust insider threat programs, this informal approach to identifying and assessing immediate concerns is greatly enhanced by in-house experts in behavioral science, threat assessment/threat management, law enforcement and counterintelligence. These in-house experts or subject matter experts (SMEs) assist component hubs in understanding the context, determinants and motivations of a person's behaviors through case conceptualization, education and mitigation strategies.

In fact, informal conversations, consultation and collaboration are often approaches that SMEs may recommend for gaining insight into an individual's reasons for behaving a certain way, their current state of mind, and how they may perceive a certain situation.

However, gaps in information, understanding and best practices persist and raise questions that require innovative answers and action. For example, how do insider threat and security professionals in the smaller components or "hubs" find additional resources and necessary guidance, especially in the more complex and concerning cases?

Additionally, where can professionals in the smaller DOD hubs find access to a team of subject matter experts in one venue, available to discuss their insights and best practices in order to determine the scope, intensity and possible consequences associated with a potential threat? Where can they share concerns and information while collaborating informally with insider threat professionals from throughout DOD who may have encountered similar scenarios?

A unique team of insider threat experts open for "office hours" would be the ideal resource. On Jan. 19, 2022, that resource became a reality when DCSA launched a new and innovative program called 'Subject Matter Expert Office Hours' through the DOD Insider Threat Management and Analysis Center (DITMAC)'s SMEs. Prior to this, hubs would reach out for consultation on cases of concern when they would arise.

However, this newly developed forum has created an opportunity for ongoing informal discussion regarding their insider threat cases and concerns for an hour-and-a-half and longer when necessary during conference calls held on a regular basis.

The team of four insider threat assessment experts, comprising a law enforcement and counterintelligence expert; a threat assessment and threat management advisor; and two senior behavioral science advisors have been providing consultation, assessment and mitigation strategies to insider threat and security professionals on a regular schedule ever since.

"Our customers can run a scenario by our SMEs and their colleagues at other hubs who may have encountered a similar situation but more importantly, they can find out if their colleagues ever implemented a mitigation strategy to help the at-risk employee," said Owen Simpson, chief of Analysis and Mitigation at the DITMAC.

Threat assessment — whether a formal process or informally via SME Office Hours — is a unique discipline requiring a team of individuals to assess an individual and determine the scope, intensity and possible consequences associated with a potential threat. The assessment is based on behaviors, not profiles; and behaviors are variable and complex in nature. The ultimate goal of

a threat assessment is to prevent an insider incident, whether intentional or unintentional.

The 'SME Office Hours' team consulted with a handful of participants on the first and second conference calls, but attendance has grown significantly to around 20 to 30 participants per session, based on consistent email messaging and word of mouth promotion.

"The potential impact has been great. It's been a true force multiplier within the enterprise because it allows for a community of insider threat professionals to come together," said Simpson. "They can exchange best practices and lessons learned. It's done through the facilitation of DITMAC subject matter experts who lend their expertise, knowledge and consultation to these different hubs and insider threat programs, especially when they present a scenario that needs to get addressed by a hub, or they just want to exchange ideas and thoughts. The SMEs have been a wonderful asset."

The DITMAC addresses and analyzes information from multiple sources on concerning behaviors and any risks that could potentially harm people, resources and capabilities. The DITMAC provides the DOD enterprise with a capability to identify, assess and mitigate risk from insiders while managing unauthorized disclosures and integrating, maturing and professionalizing counter insider threat capabilities.

"The team in our new SME Office Hours program are a professional soundboard for these insider threat programs, so it's really helped us as a community - as an insider threat professional community," said Simpson. "It's created this connective tissue among the different hubs and programs to help exchange ideas and share best practices about potential mitigation strategies."

Dr. Lindsay Braden, a senior behavioral science advisor on the SME Office Hours team, emphasizes that the conversations are intended to be very informal so people can talk through the challenges that they're facing.

"It's a huge value added, especially the networking as the hubs get to know people from the other hubs who may have similar situations," said Braden. "It's growing; we've had more and more people calling in with each iteration and they've become more comfortable reaching out to us when different issues arise."

The hubs are also reaching out to provide Braden, Simpson and the SME Office Hours team with feedback about the program.

"This is a great awareness tool at the hub level so people can learn from the larger community. Our agency is fortunate because we have a very active hub with a lot of local participation, but not everybody has a mature program," said an insider threat professional from a DOD component. "I know not everyone is aware of the resources DITMAC can provide or how easy it is to engage with DITMAC, refer a case, and share threats with the community. Others may not have skills developing local resources. While participation may vary and it will take time for people to get comfortable participating in this new virtual community, it is definitely a worthwhile resource to develop. Thanks for starting and continuing SME Office Hours."

Indeed, DCSA and DITMAC leaders and analysts plan to continue the program as an informal consultation resource that DOD components can rely on prior to, in addition to, or in the aftermath of a potential formal threat assessment.

"It's key for us to maintain an informal consultation. There are so many formal processes in place already and we want people to feel comfortable coming with questions and apparently they are," said Braden. "The questions and what we tend to talk more about focus on behavioral health concerns. The sessions are absolutely helping hubs to effectively deal with challenges related to employees exhibiting concerning behaviors. In some discussions, we've encouraged the hubs to report the challenges as cases."

ODNI Principal Deputy Director's DCSA visit concludes with 'Fireside Chat' on Trusted Workforce, diversity, DNI's mission

By John Joyce
Office of Communications and Congressional Affairs

How does the Office of the Director of National Intelligence (ODNI) — the security executive agent for national security clearances — view the implementation of Trusted Workforce (TW) 2.0 and its importance to national security?

It was one of many questions Dr. Stacey Dixon, Principal Deputy Director of National Intelligence, contemplated at a 'fireside chat' with DCSA employees during a visit to the headquarters in early May. The 'chat,' held in person and broadcast to the wider agency, included an audience of background investigators and adjudicators who will be directly affected by the new personnel security regimen.

The moderator's second question quickly followed: How do you see DCSA's role in TW 2.0 in the future?

The audience didn't have to wait long for enlightening and encouraging answers. Dixon responded in thoughtful measured fashion to questions on TW 2.0 and about a dozen inquiries ranging from her views on diversity and inclusion to how the Intelligence Community is adjusting to deal with current threats.

"We now have tools and capabilities in the form of technology that can help us. It's necessary that we make these investments," said Dixon, regarding the TW 2.0 reform effort that transforms the personnel vetting process and realigns it as one, government-wide system to enhance security while allowing reciprocity across organizations. "What we've been able to do so far is very good — there's a lot more people enrolled in the Intelligence Community as well as other parts of government and DOD in systems that are really helping us transition from the periodic reinvestigation cycle to continuous vetting."

The continuous vetting within TW 2.0 will fully replace periodic reinvestigations by employing a full suite of automated record checks, time and event-triggered activities, and analysis of agency-specific information through the National Background Investigative Services (NBIS).

"For the future — we just need to continue our ability to adapt," said Dixon. "We must get systems to move faster and that often means acquiring assistance and data while bringing people onboard — we need to do it rapidly, which is why a lot of the activities you are impacting are part of the Trusted Workforce 2.0 effort to redo and rethink personnel vetting. It's so important."

PDDNI, in her Performance Accountability Council (PAC) security executive agent role, is one of the principals continuously advising DCSA on Trusted Workforce plans and policies. "As a PAC principal, we keep up with what Trusted Workforce 2.0 and DCSA is doing for the community," said Dixon regarding the role of PAC, which includes the Office of Personnel Management director as the suitability and credentialing executive agent, the Undersecretary of Defense for Intelligence and Security, and the Office of Management and Budget's deputy director for management as principal members. Their guidance and collaboration with DCSA resulted in the risk-reducing phased approach of TW 1.25 and TW 1.5 as the TW 2.0 personnel reform effort is implemented government-wide, overhauling personnel vetting and benefitting many of those who are vetted in the process.

"We are moving towards TW 2.0 from every level, and I love the way we're talking about it now — reciprocity of the transfer of trust enabling efficient employment changes between organizations. It's the right conversation to be having and the role that you are all going to play and are playing to develop this system and roll it out is extremely important."

Dixon was also asked her views on how the ODNI has evolved since its establishment in the wake of the terrorist attacks of Sept. 11, 2001, as well as where she sees the organization going in the next 20 years.

"The 9/11 Commission said that the U.S. Government had gaps in the sharing of information," Dixon recounted. "We had seams between domestic and international systems.

Principal Deputy Director of National Intelligence Stacey Dixon (left) walks with DCSA Director William K. Lietzau at the start of her visit to DCSA. (DOD Photos by Christopher P. Gillis)

Information that resided in different places could have helped us thwart those attacks, and at that time, those individuals weren't talking to each other. Information was not being made available to do something about it — that is why ODNI was created."

The Intelligence Reform and Terrorism Prevention Act of 2004 established ODNI and since it began operating in 2005, the agency has led the Intelligence Community in intelligence integration to enable delivery of the most insightful intelligence possible.

"We are helping to integrate intelligence across all the different communities by developing information for policymakers that is better — more coherent, insightful, timely, relevant and accurate," said Dixon. "In the next 17 years, we will continue with that integration mission and mantra."

The former National Geospatial-Intelligence Agency (NGA) deputy director — a 2022 Wash100 Award winner for her leadership at NGA and ODNI to drive innovation for the Intelligence Community in geospatial intelligence capabilities, commercial remote sensing satellites, and a comprehensive science and technology strategy — cautioned that times have changed since ODNI's origin. "It's not likely that the same problem regarding the lack of interoperability and information sharing will reoccur. We figured out how to prevent some of those things from happening again. However, we have a new challenge: How do we figure out how to prevent the next one?"

ODNI is responding to that challenge by continually working on ways to prevent any potential attack against the United States by doing things that no one agency could do on its own, such as integrating the archipelago of information technology infrastructures into a single Intelligence Community IT enterprise and addressing whole-of-government strategic operational planning and information sharing to counter terrorism.

"It isn't so much that you've got agencies holding data that they're not sharing with each other," said Dixon. "Now, there is so much data out there that information is hidden in the data that you need to tease out. So, our intelligence integration mission continues at a different level, on a different scale. One of the things that is really good is our collaborative approach. There is no big stick at ODNI. A lot of what we do is due to coalitions of the willing."

Dixon emphasized that diversity is vital to successful coalitions and collaboration at ODNI and across the Intelligence Community.

"Mission success is doing what needs to be done to keep this country safe — providing the policymakers with the

"We are helping to integrate intelligence across all the different communities by developing information for policymakers that is better — more coherent, insightful, timely, relevant and accurate. In the next 17 years, we will continue with that integration mission and mantra."

information and intelligence they need to make good policy that helps move forward the interests of the U.S. and our allies," said Dixon. "In order to do so, we need to understand more of the world. We need diverse perspectives brought to the table so we can continue to innovate and bring forth new and great ideas that are going to help us to collect and analyze that information better."

The integration and analysis of information from myriad perspectives are key to ODNI's ability to ensure national policymakers receive timely and accurate analysis from the Intelligence Community to make educated decisions.

"That's what success looks like — the ability to achieve our mission in a way that keeps us ahead of our adversaries and keeps us in our place in the world as leaders," said Dixon. "We will continue to change with people at the table who have different backgrounds, upbringings, and ways of thinking about problems. We need that because the challenges will continue to keep coming at us. Future challenges will be more complex, and we must continue to generate great ideas. To me, success is having all those ideas at the table, and we must not be afraid to bring them up — to share them and know they will be valued, no matter where they're from or what they look like. That's what success looks like."

The PDDNI's visit began as DCSA Director William Lietzau and Deputy Director Daniel Lecce joined the agency's mission leaders to brief Dixon on DCSA and its mission centers: Industrial Security, Counterintelligence, Personnel Vetting, National Background Investigative Services, and the DCSA Program Executive Office with its portfolio of enterprise-wide IT programs to better serve DOD, government, and cleared industry.

Principal Deputy Director of National Intelligence Stacey Dixon (right) answers a question during the agency Fireside Chat, while moderator Cindy McGovern, Office of Communications and Congressional Affairs, looks on

Ceremony transfers DITMAC System of Systems and NISS charters to new program leadership

By John Joyce
Office of Communications and Congressional Affairs

The Defense Counterintelligence and Security Agency (DCSA) recently held a Program Executive Office (PEO) Charter Ceremony to transfer the charters of two programs impacting national security to new program managers.

The PEO Charter Ceremony comprised Change of Charters representing the DOD Insider Threat Management and Analysis Center (DITMAC) System of Systems (SoS) Program and the National Industrial Security System (NISS) Program.

"When we think about acquisition programs, we think about significant capabilities that affect warfighting and national security and that's what we're talking about today," said DCSA Program Executive Officer (PEO) Terry Carpenter at the May ceremony. "Whether it be the security of people, weapon systems, what our warfighters carry out on the front line — or what we need to accomplish to protect our way of life and democracy in the United States — these programs you will hear about really do impact national security."

During the ceremony, Carpenter presented outgoing DITMAC SoS Program Manager Charles Washington with the DCSA Director's Achievement Award for significant contributions to DCSA from January 2018 to April 2022.

"Mr. Washington successfully assisted the DOD Insider Threat Management and Analysis Center in furthering the ability to expeditiously identify and track the insider threat portfolio and facilitating protection of our nation's employee and DOD equities," according to the citation read by the ceremony's moderator. "His work across the DOD and Intelligence Communities secured innovative capabilities to expand and streamline DITMAC requirements."

Before serving for more than four years as the DITMAC SoS program manager, Washington supported various organizations as a government leader in the information technology field.

Carpenter presented outgoing NISS Acting Program Manager Christopher Carrigan — who also served as the Cloud Services and Data Management (CSDM) program manager — with the DCSA Exceptional Service Award for sustained exemplary service to the agency from September 2018 to May 2022. Carrigan — known as a technological visionary with the knowledge and intuition to lead change — joined the former Defense Security Service (now DCSA) in September 2018. He previously served as an information technology specialist at the Defense Information Systems Agency for five years within the agency's cyber directorate.

"During this time period, Mr. Carrigan distinguished himself by demonstrating unparalleled program leadership and extraordinary record of achievements as the chief architect and driving force behind the creation of the DCSA CSDM program," according to the citation. "He continuously identified ways to improve operations that led CSDM to becoming one of the most transformational programs within DCSA. His rapid establishment of capabilities and cross-functional group of experts provided internal and external tenants with Cloud Services and Big Data Platform options, supporting all facets of the DCSA mission."

At that point, Carpenter executed the change of charters between the outgoing and incoming program managers.

First, Washington relinquished his charter to Carpenter who, in turn, presented it to Erin Lambert as the new program manager of DITMAC SoS — an enterprise level capability for managing and analyzing insider threat information. The program currently supports 43 DOD components and is the primary tool for capturing, consolidating, storing, analyzing and managing insider threat data. Lambert takes on a new responsibility as DITMAC SoS program manager after serving myriad positions within a U.S. Navy PEO, including her tenure as assistant program manager for the Navy Electronic Procurement System under the PEO Manpower, Logistics,

> When we think about acquisition programs, we think about significant capabilities that affect warfighting and national security and that's what we're talking about today
>
> ***~ Terry Carpenter***

and Business Solutions within the Naval Warfare Information Systems Command.

Next, Carrigan relinquished his position as the acting NISS program manager by handing his charter to Carpenter who, in turn, presented it David Drys, designating him as the new NISS program manager.

NISS is the DCSA System of Record for industrial security oversight accessible by industry, government, and DCSA personnel. It modernized the National Industrial Security Program information environment to provide government and industry stakeholders with a data-driven, collaborative, integrated capability to assess and mitigate risk. Drys begins to lead NISS as its program manager after a career that included U.S. Navy active duty service from 1997 to 2004 and service in various positions within a U.S. Navy PEO.

"As a program manager, you maintain the perspective in managing programs and will report directly to the program executive officer," the ceremony's narrator stated after each new program manager received their respective charters. "Among numerous other duties, you will keep the leadership fully informed of program status and report any matters that could affect DCSA's ultimate commitment to the program."

Program managers — under the supervision of the PEO and the component acquisition executive — are responsible for planning acquisition programs and preparing to meet key objectives while implementing approved acquisition and product support strategies.

As DCSA PEO, Carpenter oversees a portfolio of enterprise-wide information technology programs for the development and delivery of innovative information technology solutions, advancing DCSA's broad-spectrum national security capabilities.

DCSA Program Executive Officer Terry Carpenter (left) presents outgoing Program Manager Charles Washington, Program Executive Office (PEO) with the DCSA Director's Achievement Award for significant contributions to DCSA from January 2018 to April 2022. (DOD Photos by Christopher P. Gillis)

Carpenter (left) presents outgoing Acting Program Manager Christopher Carrigan, PEO, with the DCSA Exceptional Service Award for sustained exemplary service to the agency from September 2018 to May 2022.

Carpenter (left) presents incoming Program Manager Erin Lambert, PEO, with the charter for the DOD Insider Threat Management and Analysis Center System of Systems.

Carpenter (left) presents incoming Program Manager David Drys, PEO, with the charter for the National Industrial Security System

DCSA predicts industry's annual security clearance requirements via PSI-I data collection

By John Joyce
Office of Communications and Congressional Affairs

Why did the DCSA Personnel Security Investigations-Industry (PSI-I) Program Office ensure that an electronic survey completed by parents across the country in March and April 2022 on behalf of their children was easy to complete and submit without any glitches, delays or hang-ups?

There is one very good reason — national security. These parents did not submit a survey in regards to their children's school, college or a summer camp. They responded to an important DCSA survey related to personnel security investigations.

Corporations such as Lockheed Martin, Northrup Grumman, Raytheon and General Dynamics are the 'parent' defense contractors. The 'children' comprise the many individual cleared facilities in various locations the parent companies choose to include in the survey. That is, unless a facility security officer (FSO), an assistant FSO or another security official representing each 'child' fills out and submits the report via the National Industrial Security System (NISS) themselves.

Chris Pirch, a data analyst with the Office of the Chief Financial Officer, analyzes the survey submissions from thousands of cleared contractors in order to project PSI-I requirements each year.

"We went through the survey, entering data as a parent for a child to ensure a seamless process while troubleshooting to make sure all the kinks were worked out in NISS for parents who submit consolidated reports listing all of their children facilities," said Pirch. He explained that medium and larger companies may save time by responding on behalf of their individual facilities — in some cases dozens to a hundred satellite operations authorized by DCSA as cleared facilities.

In 2022, the data collection for PSI-I projection requirements was open from March 8 to April 22 through the NISS submission site. Annual projections acquired from industry through this collection are a key component in DCSA's program planning and budgeting for National Industrial Security Program (NISP) personnel security clearances for industry.

Industry began submitting PSI-I data collection surveys to DCSA via NISS in 2019 when NISS became the system of record for facility clearance information, replacing the Industrial Security Facilities Database and Electronic Facilities Clearance System legacy systems.

Pirch credits the agency's NISS information technology experts and the DCSA Knowledge Center with resolving latency issues experienced by industry FSOs and security professionals across the country during the first year that PSI-I data collection surveys were conducted via NISS.

"Our NISS team is responsible for a lot of the good changes," said Pirch while pointing out that the system was not fully optimized and many facilities were not enrolled in NISS during its first year.

"We collaborated with our NISS colleagues to test, evaluate and improve the system for industry," said Pirch. "While testing the survey in NISS, we ensured it could be completed in as many different ways as possible. For example, we allow a corporation like Lockheed to submit one survey on behalf of all their companies, which saves them a lot of time. Instead of 100 different people — one FSO at each facility submitting a survey - they can complete a huge survey and submit it to us. It adds some complexity to the way the survey is analyzed."

Rather than submit a consolidated response for all of their children facilities, a company can choose to submit a single

> **We went through the survey, entering data as a parent for a child to ensure a seamless process while troubleshooting to make sure all the kinks were worked out in NISS for parents who submit consolidated reports listing all of their children facilities,**
>
> ***~ Chris Pirch***

response for each child facility and, of course — just like humans — there are corporations, especially small and medium size firms, who don't have children and submit a single response via NISS.

"Our industry partners' ability to quickly and easily complete the PSI-I survey is essential to the overall DOD mission and ensures a continued trusted workforce is upheld," said Britny Paynter, NISS product owner and functional manager. "We are delighted with the collaboration across DCSA mission areas and look forward to the continued support with the PSI-I team for years to come."

Since 2019 when the initial survey capability deployed, the DCSA Industrial Security Directorate (ISD) Systems Management Branch (SMB) — namely, Paynter and her colleague, Larissa Caton — worked closely with the PSI-I team to enhance the overall user experience and streamline the survey.

It required moving the survey from a manual process to an automated process, significantly reducing the burden of previous survey execution.

"When the survey first migrated to NISS, we met with PSI-I stakeholders to gain a holistic understanding of the inner working and purpose of the survey," said Larissa Caton, ISD SMB requirements manager. "Once that knowledge was baselined, we continued the collaboration with PSI-I stakeholders to further refine and develop the functionality required to enhance the execution of DCSA's PSI-I mission through the facility clearance (FCL) system of record."

Entities — including companies and academic institutions — engaged in providing goods or services to the U.S. government involving access to or the creation of classified information may be granted an FCL. DCSA processes, issues and monitors the continued eligibility of entities for an FCL.

The refining process to improve the agency's Personnel Security Investigations mission involved data collection, troubleshooting of user issues, training material and continued enhancement of the survey technical tool. Each year — after the survey closes in April — Caton and Paynter collect and polish raw data from the NISS database and provide the information to the PSI-I team for further analysis and delivery to necessary stakeholders outside of DCSA.

They also provide basic survey data, including number of submissions, when required throughout the collection period.

"In preparation for the next year's survey period, we engage with the PSI-I team — usually mid to late summer — to gather and incorporate end user feedback received in the previous reporting period," said Caton. "We encompass this feedback in our development process for NISS for deployment before the next survey goes live."

For example, when the survey went live in 2019, access to the projection table —where users input most of the data — was a multi-click process that increased survey completion time. In successive years, ISD worked to improve the latency of the overall system while reducing the amount of 'clicks' necessary to input information in the PSI-I survey. In the latest iteration of the survey, users were able to directly input data in the projection table without having to click additional pop-up windows outside the general survey landing page.

The survey is not mandatory but DCSA highly encourages industry to respond via notifications released through NISS, news releases and social media in addition to directly contacting FSOs.

"We don't want to underestimate the need for security clearances and be underfunded for any requirement," said Pirch. "A good response from industry to our PSI-I data collection survey will ensure that we are fully funded to investigate and adjudicate security clearances required for the number of engineers industry needs to work on a project. For instance, if the clearances can't be approved on time, there will be backups in the clearance process that could delay the date a Navy warship is built or integrated with new technologies our warfighters need to fight, win and come home safely."

Underestimated PSI-I requirements would negatively impact defense contractors' abilities to fulfill their obligations under contract with the federal government.

Conversely, companies in competition against each other for defense contracts are often overly optimistic about winning those contracts. Pirch — in his role as a statistician — uses regression analysis to mathematically correct the number of projected clearances a company requires to a realistic value.

"In 2018, we saw that cleared industry projected 150,000 secret investigations but only requested 100,000 Secret clearances," said Pirch. "We used that past data to develop a regression model that projects the actual number of clearances required for all these facilities."

In effect, the PSI-I Data Collection Program enables the federal government to project the actual requirements for the trusted workforce.

"We ensure that the proper number of people have the proper level of clearances," said Patrick Young, analyst at the DCSA Office of the Chief Financial Officer. "In coordination with Vetting Risk Operations, we track when these clearances have to be renewed so the government can provide us with the necessary funding to renew the clearances. This is necessary for people to have the appropriate clearances to accomplish work for DOD moving forward. In other words, we are projecting as accurately as possible the number of clearances required for the government to continue to do things that it needs to do."

NBIS leverages unique "playground" concept to test capabilities with potential users

By Yier Shi
National Background Investigation Services

As the National Background Investigation Services Program Management Office (NBIS PMO) begins incrementally deploying new capabilities to the personnel vetting enterprise, it has built an innovative testing environment, NBIS playground, that allows users to test new features, identify requirements and learn how NBIS capabilities can support the organization's business processes.

"The NBIS playground has really been a win-win for both our stakeholders and the NBIS team," said NBIS Executive Program Manager Jeff Smith. "Not only are the users engaged earlier in the process and they can see how NBIS can support their business, these same users have played a critical role in helping NBIS capture defects sooner, better prioritize enhancements, and improve training and collaboration across all missions. We have seen tremendous benefits from adopting this concept and look forward to continuing to expand this environment to more users."

The idea of a NBIS playground was originally conceived from two main tenets of the NBIS program — that it follow an Agile software development concept and the application is hosted in a government cloud environment. These two features of the application allowed for the creation of a dynamic testing environment that can easily be updated to house the latest code delivery and new capabilities for users to engage with before it reaches full operational testing. As many of the NBIS capabilities require customized configuration of the system and its workflow, the playground environment also serves as the initial launching point for users to align NBIS configuration with their existing business processes.

Since its launch in February 2022, the NBIS playground has been successfully implemented by two internal DCSA mission owners, DCSA Adjudications and Vetting Risk Operations (VRO).

For DCSA CAS (formerly the DOD Consolidated Adjudications Facility), more than 70 users were provisioned into the playground. Over the following two months of "playing," the NBIS team worked hand-in-hand with DCSA CAS users to conduct training on NBIS functionalities, build customized configurations and workflow, and provide daily support/oversight of the team's experience in the playground. The result was a resounding success as the DCSA Adjudications team was able to test 44 business processes and identify 20 configuration gaps, seven future enhancements, 13 defects, and five items that required additional training.

"The results from our playground experience with DCSA CAS is exactly what we had been hoping to achieve," Smith said. "We don't fear the issues identified by our users in the playground. In fact, we welcome it because it is the early feedback that is absolutely critical for NBIS to deploy successful capabilities to our customers using an Agile, incremental approach."

While the NBIS team logs all results of the playground into its tracking system, there is a dedicated NBIS tiger team that supports the immediate resolution of some of the items uncovered during testing. The team held weekly office hours where all issues were discussed between the technical team, training team, onboarding team, solutions team and the users to better understand and triage issues identified. This enhanced communications between the team members led to a seamless coordination between all parties in the playground.

As a result of the successful testing with DCSA CAS, the NBIS team also began a similar process with VRO on the Continuous Vetting (CV) capability NBIS has been working to deploy incrementally. The VRO playground started at end of March 2022 and so far has 22 users provisioned in the system. The program will follow the same path and configure CV workflows to allow VRO to test NBIS capabilities with their current and future business processes. The program is hoping to see similar results in identifying gaps, enhancements, defects and additional training needs. As an additional incentive of having DCSA Adjudications in the same playground as VRO, all parties were able to start testing cross mission capabilities to further test and expand the knowledge areas for future NBIS functionalities.

The NBIS Playground will continue to be an important tool for the program and the team is looking forward to expanding on the success achieved to date. The PMO will widen its use in the near future to account for both internal and external users, including DCSA Background Investigations, Federal Agency adjudication service providers and cleared industry partners.

CDSE offers digital badging in two programs

By Natalie Perkins and Ian Bailey
Center for Development of Security Excellence

Education certificates, SPēD certifications and credentials are ideal for security practitioners who want to enhance their professional development. Certificates, certifications, and credentials are earned by completing courses and assessments for various security disciplines, and they serve as formal recognition of an individual's understanding of and their ability to apply specific foundational concepts, principles, and practices. Traditionally, a physical representation of these certificates and credentials were provided in paper form. In recent years, however, the Center for Development of Security Excellence (CDSE) has transitioned to offering electronic representations of certificates and credentials in the form of digital badges.

CDSE partnered with Credly, an end-to-end solution for managing digital credentials, to provide digital badges for Security Professional Education Development (SPēD) Certifications and American Council on Education's (ACE) credit-recommended courses. Through this partnership, students are able to access their transcripts and visit the ACE CDSE webpage to check if they have any eligible courses for digital badges.

ACE is a membership organization that mobilizes the higher education community to shape effective public policy and foster innovative, high-quality practice.

ACE CREDIT connects CDSE workplace learning with colleges and universities by helping employees gain access to academic credit for formal courses and examinations taken outside traditional degree programs. ACE Credit recommendations allow students to transfer credit earned from approved courses toward completion of degree programs

Why digital badges?

Digital badges are more beneficial alternatives to physical certificates and credentials and provide the following benefits:

- Helps students gain recognition by allowing them to easily display and share their achievements in e-mail signatures, digital resumes, and/or social media sites such as LinkedIn, Facebook, and Twitter
- They are available online, and the detail behind each badge allows others to see what was accomplished to earn the award
- Provides verified digital recognition for acquiring new skills
- Allows hiring managers to easily validate acquired competencies
- Third parties can verify the status of credentials in seconds online

CDSE SPēD certification program transitions to digital badging

On June 1, 2020, CDSE transitioned from mailing its SPēD Certification Program's certifications and credentials to offering them as digital badges

With the CDSE SPēD Certification Program offering its certifications and credentials as digital badges, it minimized costs and allowed SPēD candidates to receive their certificates at a faster rate.

Digital credentials are awarded to certificants as proof that they have been conferred a SPēD certification or credential. Upon successfully passing and being conferred a SPēD certification, the certificant will receive a digital badge within 48 hours, and their digital credentials will be provided through the Credly website.

As of April 12, over 9,700 digital credentials have been issued; 7,395 accepted; 6,538 shared; and 11,615 views.

Once the certificant has accepted and claimed their digital badge, they are able to share it from Credly to their social media platforms (e.g., LinkedIn, Twitter, and Facebook) and via email. Also, the certificant can download a free printable version of their badge, and embed their digital badge on a personal website.

The *CDSE SPēD Certification Program* is part of the DOD initiative to professionalize the security workforce. This initiative ensures there exists a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals.

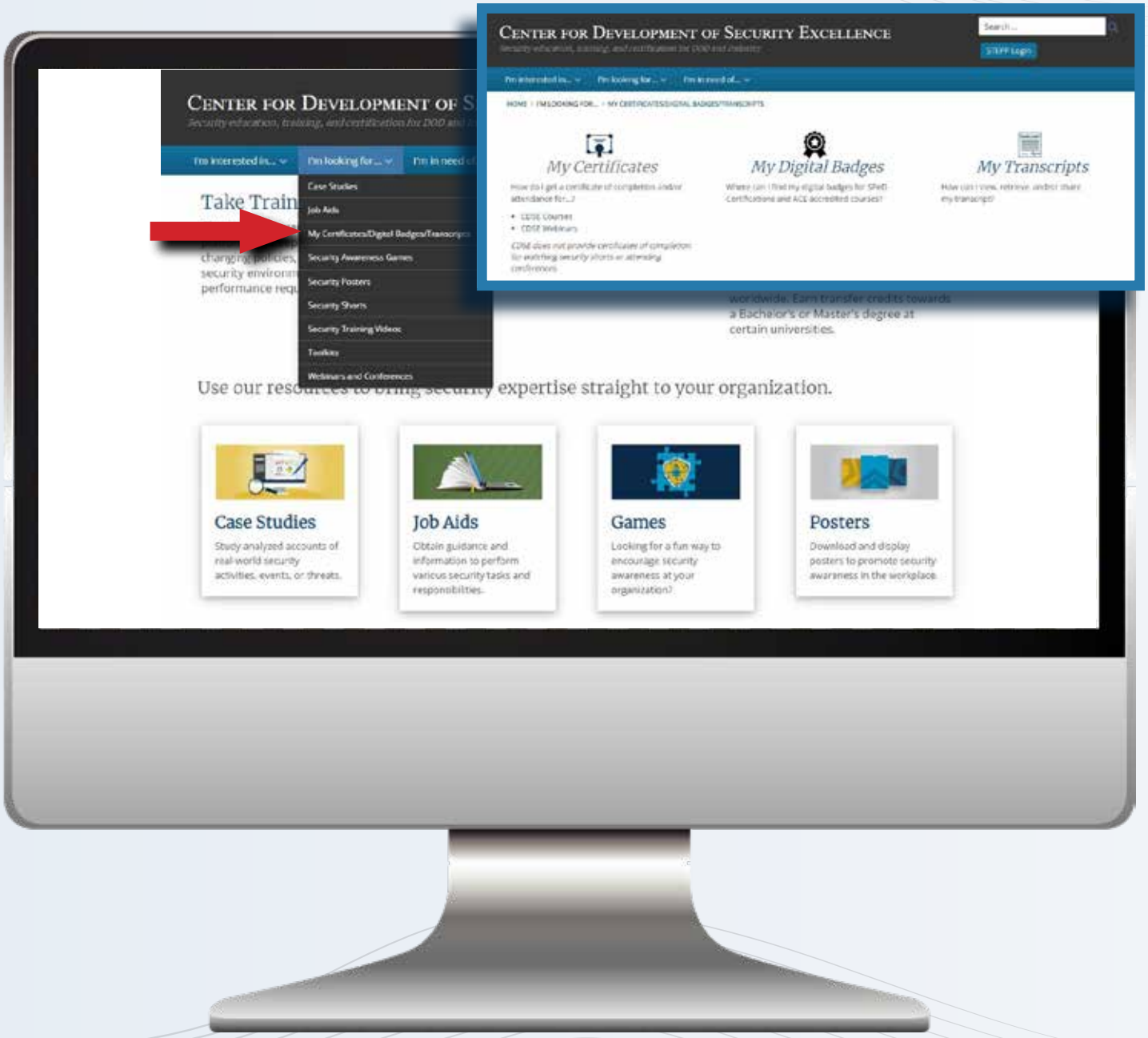
CDSE launches ACE digital badging program

In March 2022, CDSE launched the CDSE Digital Badging and Transcript Service for courses with ACE College Credit Recommendations. CDSE will now automatically confer digital badges for ACE credit-recommended courses recorded in STEPP. Upon conferral, individuals will receive an email from Credly giving access to the newly earned digital badge. This process normally takes several days. To receive a digital badge for any ACE credit-recommended courses recorded in STEPP prior to the program launch, students will need to submit a request to the USALearning Help Desk. To facilitate the process, visit the **My Digital Badges webpage** for information and instructions.

In support of the ACE Digital Badging Program, CDSE created new My Certificates/ Digital Badges/Transcripts resource pages which are accessed from the CDSE.edu homepage. These webpages contain the information regarding how to access course/webinar certificates, SPēD Certifications and ACE accredited courses digital badges, and transcripts.

To learn more about CDSE's digital badging programs

Please visit CDSE's My Certificates/Digital Badges/Transcript webpage at *https://www.cdse.edu/lm-looking-for/My-Certificates-Digital-Badges-Transcripts/My-Digital-Badges/*.



Defense Counterintelligence and Security Agency

27130 Telegraph Road
Quantico, Virginia, 22134
DCSA.pa@mail.mil
571-305-6562
www.DCSA.mil