

Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper



Volume 2, Issue 4



Directive establishing DIS in 1972 links to DSS and DCSA
50th anniversary of service supporting
national security

IN THIS ISSUE

**ASK THE LEADERSHIP:
MATTHEW D. REDDING**

**COGSWELL AWARDS RECOGNIZE
INDUSTRIAL SECURITY EXCELLENCE**

**NCCA RESEARCH TEAM:
'TALK TO THE BOT'**

IN THIS ISSUE

FROM THE DIRECTOR.....	3
DCSA CELEBRATES 50TH ANNIVERSARY OF SERVICE SUPPORTING NATIONAL SECURITY	4
ASK THE LEADERSHIP	8
AGENCY RECOGNIZES BEST IN INDUSTRIAL SECURITY WITH COGSWELL AWARDS	12
DCSA EMPLOYEES RECEIVE NCMS INDUSTRIAL SECURITY AWARDS	14
SENIOR LEADERS NAMED PRESIDENTIAL RANK AWARD WINNERS	16
DCSA RECOGNIZED WITH NCSC AWARDS IN THREE CATEGORIES.....	19
SENIOR LEADERS OUTLINE ACTIONS TO ACHIEVE STRATEGIC GOALS AT OFFSITE.....	21
NCCS DELIVERS CENTRALIZED REPOSITORY, AUTOMATES DD FORM 254 PROCESS.....	23
DCSA BEHAVIORAL SCIENCE BRANCH DESTIGMATIZING MENTAL HEALTH COUNSELING	24
VALUE OF MAKING CONNECTIONS: INDUSTRIAL SECURITY, CI AND BI GROWING STRONGER AS A TEAM.....	28
COUNTERINTELLIGENCE PUBLISHES CLASSIFIED ASSESSMENT OF THREATS TO CLEARED INDUSTRY	31
SPECIAL AGENTS SUPPORT OPERATION ALLIES WELCOME; ASSISTING AFGHAN CITIZENS RESETTLE	32
TALK TO THE BOT? COMPUTER-GENERATED AGENT ASKS QUESTIONS, COLLECTS INFORMATION FOR INVESTIGATIONS.....	34

Vol 2 | ISSUE 4

DCSA Gatekeeper

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

DCSA LEADERSHIP

William K. Lietzau
Director

John Eskelsen
Chief, OCCA

Cindy McGovern
Managing Editor

Elizabeth Alber
Editor

John J. Joyce
Staff Writer

Christopher P. Gillis
Digital Content Specialist

Tony Trigg
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

Fifty years ago, on October 1st of 1972, the Defense Investigative Service (DIS) was established “to provide DOD components and other U.S. government activities, when authorized by the Secretary of Defense, with a single centrally directed personnel security investigative service.” That mission was expanded and temporarily reduced over the years, as parts of DIS were shifted to other organizations or vice versa. The Agency’s name was periodically changed, but the net result is that the Defense Counterintelligence and Security Agency has clearly become the premier Federal security organization, supporting more than 100 Government activities in addition to the Department of Defense and with the notable addition of the critical mission areas of industrial security, counterintelligence, security training, and other aspects of personnel security.

In this regard, October 1st marked another anniversary for DCSA; it has now been three years since the newly named agency absorbed the majority of employees and resources from the Office of Personnel Management (OPM) and consolidated security mission elements from other parts of DoD. Each of DCSA’s constituent organizations have proud histories. For example, the DoD Consolidated Adjudications Facility would have celebrated its tenth anniversary

this year. The National Background Investigations Bureau, which was formed six years ago, can trace roots for some components of its vetting mission back more than a century to the early years of the U.S. Civil Service Commission—the predecessor of today’s OPM. The National Industrial Security Program was established in 1965 and transferred in 1980 from the Defense Logistics Agency to what is now DCSA. A complete timeline would portray a composite agency with multiple organizations that came together to form the agency we are today.

A complex agency with many proud histories, DCSA stands on the shoulders of American patriots who were dedicated to this nation’s security over many years. But every DCSA employee today can be proud of the fact that we carry on the great work of our predecessors. Since October 2019, when the DCSA of today came together, mission performance across the enterprise has improved substantially due to the hard work of our dedicated workforce. The decision to bring various components together yielded unprecedented success and surpassed expectations of even the most optimistic observers. We have reduced the investigations inventory and lowered costs, while at the same time improving timeliness and the trustworthiness of our workforce through a continuous vetting model that is addressing issues as they happen, years before a periodic reinvestigation would have found them. We are delivering consistent releases for the National Background Investigation Systems and operationalizing its capability. Industrial security is finding and correcting security vulnerabilities

in record time, counterintelligence professionals are far out-pacing their contemporaries in products and analytic work, and the security training directorate has drastically increased its output while maintaining award-winning performance. Recognizing the pacing challenge from near-peer competitors, expanding our industrial security efforts continues to be a strategic priority as we seek to increase national attention on the program and provide leadership to the enterprise.

As we celebrate the achievements of our predecessors, this issue of Gatekeeper touches on a number of the initiatives that have made DCSA the organization it is today. In these pages you will also see a variety of issues from our close relationship with industry at the annual NCMS meeting, to the support of Unaccompanied Children and Afghan Refugees, and efforts to destigmatize mental health treatment in the security clearance process.

It is an exciting time to be at DCSA and contribute to our mission as America’s Gatekeeper. Now is the time to turn our focus forward: on this agency’s bright future and on the country we are sworn to protect.

William K. Lietzau
Director,
Defense Counterintelligence
and Security Agency

DIRECTIVE ESTABLISHING DIS IN 1972 LINKS TO DSS AND DCSA 50TH ANNIVERSARY OF SERVICE SUPPORTING NATIONAL SECURITY

By John Joyce

Office of Communications and Congressional Affairs

The Defense Counterintelligence and Security Agency (DCSA) is celebrating two anniversaries in October 2022 thanks to a Secretary of Defense memorandum issued 50 years ago.

The memorandum signed by Secretary of Defense Melvin Laird established the Defense Investigative Service (DIS), which became operational on Oct. 1, 1972. DOD Directive 5105.42 designated DIS as a separate operating agency under the direction of the Secretary of Defense.

That 1972 DOD directive — authorizing a workforce of 1,750 military personnel and 1,250 government civilians to conduct all DOD personnel security investigations — has retained its unbroken authority over the course of 50 years as DIS was renamed the Defense Security Service (DSS) in 1999 and eventually consolidated with other organizations and renamed DCSA in 2019.

Hence, the agency celebrates 50 years of service while recognizing its third anniversary as DCSA — three years of transformation and consolidation with many other organizations, personnel, missions and resources.

After a half century, the agency not only retains the same charter in its evolution from DIS to DSS to DCSA, it is still responsible to the nation as its Gatekeeper for personnel security and vetting.

The founding DOD directive, also known as the “Charter for the Defense Investigative Service,” defined the DIS mission: “To provide DOD components and other U.S. government activities, when authorized by the Secretary of Defense, with a single centrally directed personnel security investigative service.”

Similar to today’s DCSA personnel security mission

encompassing security clearance investigations for military, government and cleared industry, DIS performed routine security clearance investigations for defense contractor personnel, as overseen by the Defense Industrial Security Clearance Office headquartered in Columbus, Ohio, at the time.

“DIS personnel who perform the investigative functions of the agency are known as special agents. Most are officers or noncommissioned officers of the various services,” according to an article entitled, *Defense Investigative Service Organized*, published in the Dec. 14, 1972 edition of DOD’s *Commanders Digest*. “Some are DOD civilian employees. Except for a few who occupy certain supervisory positions, military ranks or grades are not disclosed. The military investigators wear civilian clothes. Most of the investigating staff, military and civilian, have had investigative experience with the federal government or other investigative or law enforcement agencies.”

The article reported that DIS agents do not engage in law enforcement, explaining that “counterintelligence and criminal investigations will continue to be performed by the Army, Navy and Air Force” with DIS activities confined to the conduct of DOD personnel security investigations.

Such investigations included national and local agency checks and other investigative inquiries to determine the suitability of military and civilian affiliates of DOD for access to sensitive information. Investigative inquiries also involved the resolution of allegations such as the existence of criminal records, subversive affiliations and hostage situations.

In 1977, DIS was assigned the additional mission of law enforcement in detecting fraud, waste and abuse within DOD. In 1981, this mission was transferred to the Inspector General of DOD and the Defense

Criminal Investigative Service was formed under that office. DIS retained some law enforcement responsibilities concerning the unauthorized release of government information.

A decade after its founding, DIS Director Thomas O'Brien wrote about the development, progress and impact of the agency on national security in an article published in an American Society for Industrial Security magazine called Security Management.

"Gradually, over the ensuing ten-and-a-half years, DIS evolved into the complete security organization it is today. Its current mission not only includes personnel security investigations, but two other major functions as well," O'Brien pointed out in the May 1983 edition of the publication. "DIS conducts certain law enforcement investigations as directed by the Under Secretary of Defense for Policy, relating primarily to the investigation of unauthorized disclosure of classified information, more commonly referred to as leaks. DIS is also responsible for the three major programs involving industrial security: the Defense Industrial Security Program (DISP); the Industrial Facilities Protection Program, and the DOD Program for Safeguarding Arms, Ammunition and Explosives (AA&E) in the custody of DOD contractors."

Those three programs mentioned above — the DISP, the Key Asset Protection Program, and the AA&E Security Program — in addition to the Facility Clearance Program, were transferred from the Defense Logistics Agency (DLA) to DIS on Oct. 1, 1980.

The DISP established and maintained uniform standards for the handling and protection of classified information accessible to private industry. The Industrial Facility Protection Program developed and promoted physical security measures at certain key industrial facilities. The AA&E Program inspected contractors with possession or custody of sensitive conventional arms, ammunitions and explosives. The Facility Clearance Program processed and controlled industrial facilities' clearances.

By the end of 1984, the DIS workforce transformed to an entirely civilian population as military personnel gradually returned to their respective services.



Outgoing Acting Director Charlie Phalen, Chief of Staff Troy Little and Incoming Director William Lietzau during a change of command ceremony in March 2020.

Despite the escalating workload during these years, DIS sought to improve upon its contribution to national security by introducing new processes and programs. In 1981, DIS implemented a new type of background investigation — the first major change in the conduct of personnel security investigations since World War II. The most striking innovation in the new investigation was the inclusion of an interview of the "subject," which consistently led to the development of more significant information and gained widespread recognition throughout DOD.

In 1983, DIS launched a substantial program whereby periodic investigations were conducted on personnel with access to top secret information in addition to investigating those who had access to special compartmented information (SCI). This new and aggressive program was designed to detect cleared personnel who may no longer be reliable or trustworthy while deterring those who might otherwise become what we would now call an insider threat.

For almost four decades, periodic reinvestigations continued for all secret and top secret security clearance holders in DOD, government and industry until DCSA's implementation of the Trusted Workforce (TW) and Continuous Vetting programs. TW 2.0 is a whole-of-government background investigation reform effort that is transforming the personnel vetting process by establishing a government-wide

system enhancing security and allowing reciprocity across organizations.

DCSA announced on Oct. 1, 2021, that it successfully enrolled all DOD clearance holders in the Continuous Vetting Program. Now, more than four million DOD and government personnel are no longer required to submit a periodic reinvestigation to the DCSA Consolidated Adjudication Services every five or 10 years — a requirement that often involved extensive interviews with background investigators. Instead, their records are checked continuously, which enhances the trustworthiness of the federal workforce and helps them maintain positions of trust across DOD.

Security training has been an important element of DCSA since the 1970s. The Department of Defense Security Institute was established in 1972 under the control of DLA. Through a series of transfers of DOD security training mission areas, the DSS Academy was created and the DSS director was named the functional manager for DOD Security Training in December 2007. In 2010, the Center for Development of Security Excellence was established. In 2019 when DCSA was formed, the National Training Center in Slippery Rock, Pa., became part of the agency. The National Training Center — a Federal Law Enforcement Training Accreditation accredited academy — provides training for DCSA background investigators, quality reviewers and suitability adjudicators. Moreover, the National Center for Credibility Assessment — joining DCSA on Oct. 1, 2020 — conducts credibility assessment, training and education, research and development, technical support, and oversight activities for federal polygraph and credibility assessment mission partners.

In May 1993, DIS established a counterintelligence (CI) office in response to dramatic changes taking place in the defense marketplace and the need for current and relevant intelligence-threat data by the DIS workforce and industrial security managers. In addition to being a valuable resource for sharing CI experience and knowledge with the DIS workforce through training, policy development and operational support, the CI office enabled the identification and communication of threat data to industry.

In the same year, Executive Order 12829 replaced the DISP with the National Industrial Security Program (NISP). DIS immediately drafted the National Industrial Security Program Operating Manual (NISPOM), replacing the nearly 45-year old Industrial Security Manual to provide relevant information on oversight of the NISP.

The 32 Code of Federal Regulations Part 117, known as the NISPOM Rule, replaced the NISPOM 28 years later. This NISPOM federal rule — effective since Feb. 24, 2021 — implemented policy, assigned responsibilities, established requirements and provided procedures consistent with Executive Order 12829.

The agency applied myriad technological enhancements by the end of the Cold War and the emergence of the Information Age. New and emerging technology created new threats and challenges for the agency throughout its transition from DIS to DSS to DCSA. Technology also revolutionized the agency's business processes, security products and services.

For example, DSS deployed the Case Control Management System (CCMS) on Oct. 28, 1998 to



serve the agency's customers with a timely and more cost-effective way of managing personnel security investigations while providing associated products to our customers.

While it was in use, CCMS interfaced with the Electronic Personnel Security Questionnaire (EPSQ), which significantly decreased customer input and DSS processing time. EPSQ software replaced the paper format, eliminating the necessity for individuals to fill out as many as four personal history forms. This information was saved electronically for the individual's future use, eliminating the need to repeat information previously provided. A reduction in overall investigative processing time was a major benefit of the EPSQ. Fewer investigative packets were returned to the requestor for inaccuracy and because the EPSQ was automated, mail time was no longer a factor in the investigative processing time.

The technological revolution continues at DCSA. Today, the National Background Investigation Services (NBIS) is the technological capability that will enable continuous vetting within Trusted Workforce 2.0. NBIS is a secure end to end information technology infrastructure for comprehensive personnel vetting for the U.S. Government—from subject initiation, background investigations, adjudication, continuous vetting, and transfer of clearances. Mandated by Congress for enhanced cybersecurity posture, data protection, and to replace multiple disparate legacy systems, NBIS will transform the personnel vetting process to deliver improved security, more customizable solutions, faster processing, and increased efficiency while also enhancing user experience.

New and emerging technologies coupled with the agency's tradition of process improvements, cost avoidance and doing more with less also continues. DCSA's

customers are benefitting from improved background investigation products as the nation's legacy personnel vetting process is modernized and transformed. The agency's streamlined pricing structure reduced fiscal year 2021 and 2022 costs of personnel vetting products and services while costs for fiscal year 2023 will keep steady with fiscal year 2022 pricing.

"DCSA is helping our customers by reducing their costs while standardizing pricing to support predictability and enhance stability in annual and long-range customer agency budgeting," said Lietzau. "Our efforts to reform our pricing processes while implementing major change to enterprise-wide personnel vetting is paying off in cost savings for customers across government."

Over the course of five decades, the agency has evolved in response to the ongoing revolution in computing, information sharing, communication technologies and the internet that changed the nation, government, DOD and industry. As DCSA continues its transformation, it will work to proactively and positively impact national security with the most effective, timely, highest quality and technologically advanced personnel vetting, background investigations, adjudications, counterintelligence, counter insider threat, industrial security, and educational products and services on behalf of its DOD, government and industry stakeholders.



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.



**Matt Redding,
Assistant Director for
Industrial Security**

Redding is responsible for managing, directing, and coordinating the day-to-day operations of the industrial security mission. Prior to joining DCSA, Redding served as

the Deputy Director, Individual Assistance Division in the Federal Emergency Management Agency (FEMA), where he oversaw annual recovery budgets of over \$5 billion and more than 5,000 federal and contracted employees. He also served as the Director, National Integration Center and deployed to the National Response Coordination Center in support of the COVID-19 national emergency response.

Redding is a retired U.S. Army Colonel, having served 31 years. During his final assignment at National Defense University, he served as Assistant Professor of National Security and Resource Strategy, where he was asked to lead development of a new curriculum on Land Domain of Warfare. His other military assignments include Chief of Current Operations, Strategic Readiness, and Policy, U.S. Army G4, in the Pentagon; Chief of Staff, 21st Theater Sustainment Command, Kaiserslautern, Germany; Commanding Officer, 598th Transportation Brigade, Sembach, Germany; and Commanding Officer, Regional Support Command — Southwest, Camp Leatherneck, Afghanistan.

Redding received a Master's of Strategic Studies, U.S. Marine Corps University; a Master's in Supply Chain Management, Smith School of Business, University of Maryland; and a Bachelor's in Government and Philosophy, St. Lawrence University.



QUESTIONS AND ANSWERS

We have your bio, but what would you like to highlight?

The interesting thing is that during most of my military career I was the beneficiary of good industrial security programs that allowed my Soldiers and I to employ weapons and military systems in combat that gave us significant overmatch against the enemy forces we faced. I never questioned that the gear and tools we used were the best — I just never knew how they got to be so good for such a long time. In my final years in the Pentagon and as a War College instructor — I came to grips first hand with the “how” to protect this overmatch, and how complex the acquisition and sustainment cycles of our industrial base were as we planned for and prepared for global contingencies under the new “great power competition model”. My experience in large scale acquisition and logistics along with my recent current operations roles in FEMA have made me realize that this is the place folks want to be if protecting the nation is their life's calling.

What brought you to DCSA?

I was fascinated by some of the transformation efforts that I had watched from a distance as I worked at FEMA. My own security clearance had been recently adjudicated in record time and I studied the progress the agency had made in bringing down those timelines to the current levels. I also had to keep my finger on the pulse of industry because FEMA relied so heavily on similar acquisition and industrial base issues during our national COVID response. When I saw some of the enduring threats posed by our adversaries I wanted to get back into the “fight” and stand a post. The urgency and need for a long range view of industrial power had been a passion project for me in the military, and when I was at FEMA I saw firsthand the strengths and vulnerabilities on full display with regard to production, labor, and mobilizing capital funds in our economy.

What are your priorities for Industrial Security?

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 Counterintelligence (CI) support.

Directorate personnel conduct CI functional services within cleared industry through CI awareness briefings, travel pre- and de-briefs, and the collection of Foreign Intelligence Entity 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?

Our priorities are pretty simple: We have to invest in our human capital and retain security professionals. This will then allow us to focus on current threats to the industrial base for which DCSA has oversight responsibilities. This includes as a major part of our mission ensuring contractor compliance with their contractual requirements for the protection of classified national security information and implementing our mission of oversight of associated controlled unclassified information. Finally, having 21st century technology will enable our personnel to better analyze, mitigate, and identify threats to cleared contractors and within our other non—NISP mission areas. These three priorities will drive our efforts across the next three to five years as we seek to emerge from the COVID operating environment.

What are the biggest challenges facing Industrial Security?

The biggest challenge is that China and our other adversaries are using legitimate and quasi-legitimate means to steal industrial and academic research. The fact that we live in a free and open society is our biggest strength but where this open environment allows for rapid and exciting opportunities to innovate, develop economic and technological advantages, it can also be exploited. We are finding more and more complex company structures and financing arrangements these days and making sure that threat actors don’t have significant Foreign Ownership Control or Influence (FOCI) is a heavy analytic lift given the global nature of the economy and capital markets.

We need to meet this challenge with enhanced oversight and a “back to basics” approach to compliance based security measures where personnel security, threat information, physical and cyber security converge at the point of production or access to classified information at cleared facilities where DCSA is the cognizant security authority. We trusted cleared industry to maintain strong security protocols through the COVID period of operations and we are surging back out to industry sites to begin again the process of formal security reviews and cyber compliance inspections. We are deepening our analytic capability to track FOCI factors and seeking to magnify our security professionals with new tech and analytic tools to rapidly detect influence or individuals who might be targeting specific national capability.

Integrating these new tools with our existing and future workforce is urgent and difficult. We will need to keep a focus on our ability to invest in security training and the modern practices of our field representatives and expand our influence by keeping industry and other security professionals in the NISP to help us provide “gatekeeper” functions.

You have had several meetings/engagements with Government Contracting Activities (GCAs) and the acquisition community. What do you hope to achieve with these meetings?

These have been exceptionally helpful meetings and what I have learned is that security policy needs to better align against our information policy and acquisition policy. Acquisition policy and information and technology standards are all governed by separate and closely related regulations. I am seeking to get security language better nested in these regulations and help clarify how the department oversees information. Better alignment and coordination can make each stronger so that when contracts are made — I think we have to better understand how the “wheel of time” affects each regulation because our adversaries are not tied to a timeline of updates.

I have also seen and communicated that cost, schedule, and performance of the program need to be “refreshed” with regard to modern security practices related to technology, controlled unclassified information (CUI) and how the program maintains its classified information. I think DCSA will be able to assist the entire Department align its policy better when we can demonstrate known and suspected threats to certain programs. The GCA programs, through their Services, will need help addressing security from pre-award to full scale production of unique technology. The thought I try to leave GCA leadership with is that “DCSA is YOUR security agency” and our mission is to support their classified efforts. If security measures are well articulated in the contract then the contractor WILL do them.

I have shared with many folks that my view of Industrial Security has radically changed in the past year or so — industrial security doesn’t work “overnight” rather, it works “over time”. I think evidence of this is playing out daily in Ukraine where U.S. weapons are turning the tide of battle with missiles, artillery, drones, and rocket artillery that has been protected across multiple decades because the “secret sauce” was protected properly from the beginning of the program. I am actively seeking ways to collaborate with GCA’s, military departments and agencies like DCMA, DARPA, and DLA to help them see the threats — and then ask for their help in taking measure inside their authority to address the threats.

You have also had several meetings/engagements with field personnel. What have you learned from them?

No matter who I speak with in the field — I have been impressed by the quiet and humble professionalism that everyone in DCSA has displayed no matter if they are a Background Investigator, Industrial Security Representative, Information System Security Professional, Counterintelligence Special Agent or our headquarters analytic team, everyone makes me proud to be an American.

The main thing that I have picked up on is the need to provide better oversight and coordinated security reviews. I think our folks across the board are finding places where COVID didn’t affect security too much — but where it did — there are some significant problems and the pressure to fix and continue the mission is a strain on the workforce as we complete our work queue that built up from COVID. Since September 2021 the Industrial Security team has completed nearly 1,700 inspections with new ratings procedures. We found many companies that need attention and we will have to prioritize our efforts to the places needing our oversight the most. Our field workforce then will need continued support and advocacy from us here in headquarters to ensure they have good communications, solid facilities, and administrative support to do the things they need to do in the field.

Words are cheap from me — I want folks to hold me accountable to making sure we stabilize our procedures, invest in people and the education they need, and remember that this is a job that is driven by love of our country. Service to our nation has never been more important and even with my combat tours as a Soldier — the risks to global freedom and our national ethos are real.

The director has talked about a pivot to Industrial Security at the national level. What does that mean for the staff and how do you see implementation at DCSA?

I think DCSA is beginning to really find its true potential in the industrial security arena. The rapid maturity and transformation of the agency is still underway but the threats we all protect against are not slowing down. What the director has communicated with me is how the agency (and more broadly the Department of Defense) should balance its emphasis toward industrial security in a broader sense of the word. Part of that was a simple name change where our directorate used to be called “Critical Technology Protection” — but Industrial Security is broader than that in a real sense. Industrial Security involves acquisitions and mergers and corporate structure. Industrial Security involves threat finance and bold-faced, naked espionage against critical technology inside our weapons factories. Industrial security involves knowing if we can trust someone with Secret or Top Secret information — and this all comes down to the factory floor where physical security and controls allow folks to open doors and access information systems. More and more non-classified supply chains can impact classified production of weapons — and anyone who had to search for toilet paper during COVID can see how non-classified supply and demand will affect people and industrial capacity. When the director talks about a “pivot” toward Industrial Security he is acknowledging that the people, technology, and role played by our directorate and the field personnel has never been more important and we need to make wise investments in growing and sustaining this capacity to meet threats posed by nations like China and Russia.

Industrial Security oversight of industry has been compared to a pendulum with strict enforcement on one side and partnership on the other. What do you think the right balance is and how is it achieved?

This is a great question! I think much of our current situation is driven by sheer workload in the post COVID backlog of compliance work. I can't speak to the longer history or pendulum swings but have talked to previous senior leaders in both government and industry and agree there needs to be a balance. Our emphasis with the current workload is on getting back out to industry sites which haven't been visited across the COVID period and execute our oversight mission. On these missions we published new security ratings guidance, fielded user tools for industry, and with the help of our security training team, developed many new products to help industry prepare for our visits ahead of time. What many people may not fully realize is that our security oversight is “required by contract” — thus the binding contract between the company and the government to produce classified items is what we are enforcing. The NISPOM is not our requirement per se — it is required to be followed based on the contract with the government to conduct classified work. Evidence that strict compliance works is easy to find, just look at any “name brand” weapon system in the news from artillery, anti-air missiles, anti-tank weapons or drones — these are programs that have been in existence for decades and strict enforcement allowed their classified technology to “perform as advertised.” This is not to say we don't also have a responsibility to partner with industry, in providing guidance and enabling their protection programs success — quite the opposite. The director spoke recently at the NCMS conference as the keynote address before presenting the Cogswell Award to many industrial partners. He characterized them as “gatekeepers” of our nation's secrets and technological marvels. I couldn't agree more — we are partners with industry because we do trust them to do classified work — we need to help them learn and train and understand compliance measures but at no time does anyone have any doubts about whether compliance is the end state for our enterprise. We do want to partner with industry and explain and support the development of better policy — but compliance is required by law under the binding contracts companies sign.

DCSA RECOGNIZES THE BEST IN INDUSTRIAL SECURITY; 26 FACILITIES RECEIVE COGSWELL AWARDS IN 2022



On June 22, 2022, the Defense Counterintelligence and Security Agency presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 26 cleared contractor facilities, during the annual NCMS training seminar in Minneapolis, Minn. The Cogswell awards represent the “best of the

best,” and the winning facilities’ security programs stand as models for others to emulate. These 26 facilities represent less than one-tenth of one percent of the approximately 12,500 cleared facilities in the National Industrial Security Program (NISP).

“Industrial Security has never been more important than it is today. Each of these recipients show clear management and corporate

commitment for security,” said DCSA Director William K. Lietzau during the Cogswell ceremony. “But the facilities don’t create excellent programs, people do — the facility security officers (FSOs), the security staff, and the company leadership. Without their commitment and dedication, their facility would not be here today. “While the focus and accolades today are justifiably on the Cogswell

winners, I would be remiss if I did not also recognize the DCSA workforce; the industrial security representative, the information systems security professionals, counterintelligence special agents, and others spread across the country in our field offices," Lietzau continue. "They are our first line of defense and the first number or email an FSO reaches for when there is a problem. And they are as committed to security excellence as the facilities we recognize today."

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.

Congratulations to the 2022 Cogswell Award Winners!

The Aerospace Corporation
Huntsville, Ala.

Applied Research Associates, Inc. Southwest Division
Albuquerque, N.M.

Aptima, Inc.
Woburn, Mass.

Booz | Allen | Hamilton, Inc.
Eatontown, N.J.

CGI Federal, Inc.
Huntsville, Ala.

Chemring Sensors and Electronic Systems, Inc.
Charlotte, N.C.

Horizon Construction Group, LLC
Memphis, Tenn.

International Business Machines Corporation
Williston, Vt.

Kitware, Inc.
Clifton Park, N.Y.

L3 Communications Integrated Systems, L.P.
Tulsa, Okla.

L3 Harris Fuzing and Ordnance Systems, Inc.
Cincinnati, Ohio

L3 Harris Greenville
Greenville, Texas

Lockheed Martin Corporation, LM-Security Operations Center
Orlando, Fla.

Lockheed Martin-Missiles and Fire Control, Santa Barbara Focalplane
Goleta, Calif.

Prism Maritime LLC
Chesapeake, Va.

Raytheon Company
Largo, Fla.

Raytheon Company
Lawton, Okla.

Rockwell Automation, Inc.
Milwaukee, Wis.

Rockwell Collins, Inc., a part of Collins Aerospace
Cedar Rapids, Iowa

Sierra Nevada Corporation
Hagerstown, Md.

Sierra Nevada Corporation
Beavercreek, Ohio


Solipsys Corporation dba Raytheon Solipsys
Fulton, Md.

Teledyne Defense Electronics, LLC
Milpitas, Calif.


The University of Alabama in Huntsville
Huntsville, Ala.

Verity Integrated Systems
Huntsville, Ala.

Walsingham Group, Inc.
Fayetteville, N.C.



Chuck Tench, National Background Investigation Services, presents information about NBIS at the NCMS training seminar.



Mike Ray, Vetting Risk Operations, discusses Trusted Workforce 2.0 at the NCMS training seminar.

DCSA EMPLOYEES RECEIVE NCMS INDUSTRIAL SECURITY AWARDS

During this year's annual NCMS training seminar, several DCSA employees received Industrial Security Awards:

- ◆ Mike Ray, supervisory personnel security specialist in Vetting Risk Operations (VRO), received the award for his support to development of the Defense Information System for Security (DISS).
- ◆ Chuck Tench, project manager in the National Background Investigation Services (NBIS), received the award for his efforts related to the transition from the Joint Personnel Adjudication System (JPAS) to DISS.
- ◆ DCSA employees in the Controlled Unclassified Information Working Group received the award for their efforts related to the development of CUI programs.

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.

Mike Ray

Ray partnered with industry members over the last three years educating and training facility security officers (FSOs) and security staff on personnel security processes. He was a key supporter of the National Industrial Security Program Policy Advisory Committee (NISPPAC) DISS Industry Working Group in the testing and development of changes needed for DISS in support of mission requirements for industry. He worked side-by-side with working group subject matter experts to ensure industry concerns were addressed.

“My goal for the training was to educate industry on current processes and inform on new processes that will be implemented for Trusted Workforce 2.0, as well as provide job aids through the slide deck that industry can reference during the day-to-day duties,” said Ray. “It was paramount that we partner with the NISPPAC team members to understand challenges, requirements and identify solutions together that will positively impact industry as a whole. VRO works closely with the NISPPAC when implementing guidance and they always partner with us to assist with communication efforts.”

The DCSA Controlled Unclassified Working Group Mary Seibert, Industry Rep to the CUI team; Clement LaShomb, formerly of Enterprise Security Operations (ESO); Richard Rayner, ESO; Dahlia Thomas, ESO; and John Massey, formerly of ESO, acted as the DCSA Working Group Lead. Not present for the photo was Lilian Benitez, ESO.



NCMS photo by Linda Reineke

Chuck Tench

Tench has spent much of the last three years educating and training facility security officers (FSOs) on DISS functionality and use. He was a key supporter of the NISPPAC DISS Industry Working Group in the testing and development of changes needed for DISS in support of mission requirements for industry. He worked side-by-side with working group subject matter experts, NCMS and cleared defense contractors to ensure industry concerns were addressed. His dedication and commitment to resolve industry challenges improved the transition from JPAS to DISS, reducing some of the impacts to FSOs and industry organizations.

“This was a herculean effort, and there was no DISS training support as we closed in on the JPAS sunset date. With the assistance of CDSE (Center for Development of Security Excellence) and NCMS, training was developed and delivered to user communities in weekly webinars between December 2020 and March 2021,” said Tench. “The Boyers provisioning team helped with improved processes to enable industry users to obtain their DISS user accounts in an average of three days, down from over two weeks. The Customer Engagement Team formed a single point of entry for all helpdesk calls and emails related to DISS and laid the framework for the follow-on to NBIS.”

DCSA CUI Team

The CUI Working Group is comprised of DCSA civilians and contractors and NCMS members. In August 2021, the NCMS CUI Committee, led by Mark Whitteker, and the DCSA CUI Team, led by John Massey, began collaborating on a bi-weekly basis to identify the tools and resources necessary to support industry in developing CUI programs. These engagements were fruitful and collectively, they were able to develop a number of resources to support industry in their CUI program efforts.

The DCSA recipients from the CUI working group are:

John Massey, formerly of Enterprise Security Operations (ESO) within Industrial Security, acted as the DCSA Working Group Lead

Lilian Benitez, ESO

Richard Rayner, ESO

Clement LaShomb, formerly of ESO and now field office chief, Andover Field Office, Mass.

Dahlia Thomas, ESO

DCSA SENIOR LEADERS NAMED AS PRESIDENTIAL RANK AWARD WINNERS

Three DCSA senior executives were named as Presidential Rank Award Winners for 2022. Mark Sherwin, a member of the Defense Intelligence Senior Executive Service (DISES) and deputy assistant director of Background Investigations, was a Distinguished Rank recipient. Dr. Cherry Wilcoxon, a Defense Intelligence Senior Level (DISL) and formerly with the Office of the Chief Financial Officer, was also a Distinguished Rank recipient. Craig Kaucher, a DISL and senior advisor, Cyber Operations, Program Executive Office, was a Meritorious Rank recipient.

The Civil Service Reform Act of 1978 established the Presidential Rank Awards Program to recognize a select group of career members of the Senior Executive Service (SES) for exceptional performance over an extended period of time. Later, the Rank Award statute was amended to extend eligibility to senior career employees with a sustained record of exceptional professional, technical, and/or scientific achievement recognized on a national or international level. Two categories of Presidential Rank Award are available:

- Distinguished Rank Recipients are recognized for sustained extraordinary accomplishment, and only one percent of the career

SES or senior level may receive this rank.

- Meritorious Rank Recipients are recognized for sustained accomplishment, and no more than five percent of career SES or senior level members may receive this award.

In his nomination for the award, Sherwin was recognized for the following accomplishments:

- He leads operations that enable the Defense Counterintelligence and Security Agency (DCSA) to conduct approximately 2.6 million personnel security and suitability background investigations annually for 95 percent of Federal government personnel.
- With the abrupt loss of the government's largest investigative fieldwork contractor, Sherwin exercised leadership, management expertise, and innovative and collaborative approaches to problem-solving to guide more than 1,800 federal employees and 5,000 investigative contractors through that major capability gap and to eliminate a backlog of investigations that was deemed a national security crisis. This resulted in reducing the investigative backlog by 71.6 percent (from 725,000 to a sustainable, capacity-driven steady state of 206,000), improved

timeliness, and achieved cost efficiencies, resulting in the highest employee engagement and customer satisfaction scores in years.

- He built and sustained Field Operations momentum, efficiency, and workforce cohesion, despite two major externally—driven reorganizations, including the congressionally—and Presidentially—mandated transfer of the personnel security investigation mission from the Office of Personnel Management (OPM) to the Department of Defense (DOD).

- His foresight, advance planning, preparations, and deft management of a nearly \$1 billion budget mitigated impacts of the unprecedented COVID-19 global pandemic on investigative processes and continuity of operations. Field Operations promptly reprogrammed resources and pivoted to telework and virtual processes to sustain investigative fieldwork at high standards of productivity, quality, and timeliness throughout the pandemic. 5,052 VTC interviews were conducted in remote locations in FY19, with reduced temporary duty and travel costs. Sherwin's advance planning and preparations enabled investigative processes to rapidly adapt and continue uninterrupted



Mark Sherwin



Craig Kaucher

throughout the pandemic, closing nearly 2.2 million investigations in FY20 with a 99.92% rate of quality acceptance by customers.

In her nomination for the award, Dr. Wilcoxon was recognized for the following accomplishments:

- She represented the agency in internal and external stakeholder engagements to develop near- and long-term financial and resource strategies for the transfer and merger of mission and support personnel, contracts, resources, and responsibilities of the National Background Investigations Bureau, the DOD Consolidated Adjudications Facility (CAF), Defense Security Service, and other security enterprise missions and essential support functions to form DCSA. Her leadership and expertise led to a successful transfer of over \$1 billion in contracts and funding and more than 3,800 personnel into DOD's financial management systems, ensuring all transferring personnel would receive their salaries and the personnel vetting mission would continue without interruption.

- Wilcoxon established DOD's first new working capital fund (WCF) in 23 years to replace the Office of Personnel Management's \$1.6 billion revolving fund account for background investigation services. She assembled and expertly led a team of employees and contractors to develop and automate a set of business rules, establishing data input controls and standardization for DCSA to efficiently and effectively process background investigation cases and to bill and collect in a timely manner, while minimizing the resources required to perform data clean-up and reconciliation tasks.

- While others discussed but could not resolve how to invoice Federal and DOD customers for background investigation services, Dr. Wilcoxon created an Interim Customer Relationship Management solution from concept through development, ensuring end-to-end testing of a system to ingest case billing and revenue event data from the legacy OPM Personnel Investigations Processing System (PIPS) case management system

into the DCSA Defense Agencies Initiative system, using a Statistical Analysis System platform to drive results in less than 6 months.

- Wilcoxon's early and proactive engagement with stakeholders led to the DOD initiative to accelerate the end of DCSA's dependency on financial and accounting support from OPM, with the transfer (novation) of \$50 million in open legacy customer agreements and \$1.8 million in accounts receivable transactions to the DCSA financial system for an annual \$10 million cost savings to taxpayers. Leveraging her computer science background, Wilcoxon designed and implemented a business model with automated rules and standardized processes to timely bill and collect for background investigations case services, a system which reduced account delinquency rates below commercial standards and collected over \$1 billion in an 8-month period. Her efforts ensured the WCF was solvent (the only one in DOD to end Fiscal Year 2020 in the black) and led to a price reduction for all

Federal government background investigations customers, all while managing the execution of the \$2.5 billion FY 2020 budget with obligation rates of 94 percent for the background investigations WCF and 99.9 percent for DCSA's general funds.

In his nomination for the award, Kaucher was recognized for the following accomplishments:

- While the Chief Information Officer for the Defense Security Service, Kaucher led many cybersecurity enhancements and directed redesign of the agency's risk management framework approach to streamline the process, significantly reducing the timeline to one of the quickest in DOD without compromising security. He directed removal of 45 field office firewalls to mitigate unnecessary hardware outages and time-consuming upgrades, saving \$2 million. He led deployment of software to centrally manage all privileged accounts and provide insight into any changes made at the file level, and initiated foreign country internet protocol blocks of DOD adversaries. "I focused on cybersecurity when I became the DSS OCIO," he said. "I think we stepped up our game while I was there, and the team continues to do so now. I'm very proud of the team."

- Kaucher was an essential architect of the agency's planning and preparations to assume responsibility for DOD's background investigations from the National Background Investigations Bureau (NBIB) of the Office of Personnel Management (OPM), as directed by Section 951 of the National Defense Authorization Act for fiscal year (FY) 2018 and in the subsequent comprehensive redesign of personnel vetting processes.

- He was instrumental in effecting a seamless and secure transfer to DCSA of the OPM system that was center of two 2015 cybersecurity breaches, where adversaries stole sensitive information from the background investigation database. The scope of Kaucher's responsibilities increased dramatically, when OPM declared they could no longer honor their interagency agreement to manage the legacy IT system. He demonstrated exceptional technical competencies and leveraged his deep cybersecurity and technical skills to coordinate the right team of experts from IT operations, cybersecurity and systems architecture to transfer the system, designed and built in the 1980s, to secure operational effectiveness under DCSA. "We as a team were able to pivot in the middle of a year to take on the legacy BI systems and take

full ownership," he said. "It was a monumental feat on the part of a lot of people, and was a real team effort. But the people who carried the water was Acquisition and Contracting personnel carried the water because they transferred contracts in record time and made a determination of what to do with other contracts."

- Kaucher established weekly engagements with new mission partners in DCSA personnel vetting, key NBIB and OPM senior staff, and the National Background Investigation Services Program Executive Office to fully understand and address their needs, and work in close collaboration on future planning. The NBIS PEO relies on him to identify and share capabilities, requirements, and information of mutual interest and value in support of capabilities planning and development of the future NBIS. His judgment and advice are trusted and invaluable.

"In my mind, this is a team award," said Kaucher when asked what this award represents. "There's a small group of team members who have worked with me throughout the transition and they know who they are, and there's a larger team who deserves credit as well. If standing on a stage I would say, I'm accepting this award on behalf of the whole team."

DCSA RECOGNIZED WITH NCSC AWARDS IN THREE CATEGORIES

DCSA received recognition in three categories of the 2022 Intelligence Community National Counterintelligence (CI) and Security Professional Awards sponsored by the National Counterintelligence and Security Center. The award program recognizes CI and security practitioners for exceptional performance in 19 categories.

Amber Jackson, Center for Development of Security Excellence (CDSE), received the Individual award for Education and Training. Jackson became the face of CDSE Insider Threat Division, and initiated and played a pivotal role in meetings with internal and external stakeholders and partners to maintain mission momentum. This resulted in a successful National Insider Threat Awareness Month, a national campaign aimed at helping security programs detect, deter, and mitigate insider threats by increasing awareness, emphasizing reporting, and sharing best practices for mitigating risks. Throughout 2021, Jackson engaged with the Insider Threat and Security workforce by soliciting stakeholders for feedback and collaborating with partners on strategic messaging and training initiatives. Jackson delivered the Insider Threat program brief to 71 security professionals and stakeholders at the 2020 Curriculum Review meeting. The brief gave an in-depth look at the Insider Threat curriculum and products, and enabled the audience to verify that the CDSE InT curriculum met the standard for security community needs.

“My current role requires a lot of time, coordination, perseverance, and thick skin on occasion. This award confirms my professional ethos and my aspiration to always be excellent, regardless of the assignment,” Jackson said. “I also firmly believe that this award is a direct reflection of my team and organization. Yes, this is an individual award, and what I do is far from simple, but my colleagues all make it possible. Despite obstacles, and there are some outstanding ones — they deliver. All so I can deliver.”

Shawn Case, CI special agent in the Honolulu Field Office, received the individual award for Industrial Security. His innovative intelligence collection strategies and security approaches to thwarting the threat facing cleared industry resulted in disruptions to threat actors’ activities and the strengthening of relations among U.S. allies in the Hawaiian Islands, and foreign countries across the U.S. Indo-Pacific Command (USINDOPACOM).

“This award is a reflection of all the work that others and I put into aligning Department of Defense and National level strategies with DCSA’s CI support to USINDOPACOM and cleared contractors assigned and traveling across the Indo-Pacific Region,” he said. “The work we accomplished foreshadowed the 2022 National Defense Strategy and the Department of Defense’s prioritizing of threats in the Indo-Pacific region.”

Additionally, Case conceived and spearheaded numerous initiatives, to include intelligence-led, asset-driven security assessments, CI threat briefings and interviews where he identified vulnerabilities and mitigated threats with tailored countermeasures that denied the adversary from exploiting those vulnerabilities. In addition to his support of cleared facilities, he devised a comprehensive plan to directly support the effort to secure a trusted cleared workforce by identifying and providing cleared travelers a CI threat travel brief specific to the country being visited.

“This award is more about the personnel I have had the pleasure of working with, for without them, I would not be receiving this award. There are many other people within the agency who have supported me in numerous ways that have allowed me to be at the right place and right time to be successful,” Case said.

“From the CI leadership at Western Region to the CI leadership at headquarters, who gave me the trust and leeway to develop an idea and work it to fruition. And to my coworkers who helped me develop some initial thoughts from the embryonic stage to implementation. Ultimately, it’s all about the team effort. We are all in this together.”

The Vetting Risk Operations Continuous Vetting (VRO CV) Team received the team award for Personnel Security. The VRO CV team made significant advances in reforming the DOD and Federal Enterprise personnel security clearance program. The VRO implemented visionary new procedural enhancements to create a robust, timely, and multifaceted personnel clearance process that addressed emergency Trusted Workforce policy requirements. The agency’s 2021 stretch goal was to enroll the entire DOD cleared population into a CV-compliant program and to offer CV Service to other federal agencies. In order to have the appropriate bandwidth, the VRO CV team provided input into evolving TW 1.25 policy to take a risk-based approach to focus initial CV enrollment on the highest-value data sources and provided data driven input to facilitate modification of existing requirements for type and frequency of data sources required.

Members of the award-winning VRO CV team include: Ryan Dennis, William Coffey, Sarah Rivers, Erin Fitzgerald, May Wang, Megan Clapp, Nathan Tise, Michael Ray, Lynnette Weber, Janeen Beatty, Jordan Derby, Christopher Carrigan, Jack Jibilian, Timothy Miller, Emily Martin, and Sara Coonin.

SENIOR LEADERS OUTLINE ACTIONS TO ACHIEVE STRATEGIC GOALS AT OFFSITE

By Daniel J. Lecce, DCSA Deputy Director, and Juli MacDonald, Chief Strategy Office

DCSA senior leaders gathered in mid-June to begin the pivot from planning to implementation of the DCSA Strategic Plan (2022-2027). As DCSA's first five-year strategic plan, this vision for the future requires innovative ways of working together and taking action to continue agency transformation and delivery of national security missions. Senior leaders from every mission area and enterprise support office came together to discuss implementation plans to achieve DCSA's Strategic Goals and next steps for cross-cutting agency priorities.

SENIOR LEADER OFFSITE OVERVIEW

Goal Champion Presentations: The DCSA Strategic Plan has four mission goals and five enterprise goals, all cross-cutting and requiring enterprise-wide engagement. During the offsite, Goal Champions (senior leaders responsible for goal achievement) presented their implementation approaches, focusing on how the DCSA mission areas and supporting elements must transform to meet future challenges. These presentations detailed near-term executables, dependencies, risks, and requirements for success. Attendees were given the opportunity to provide constructive feedback to ensure diversity of input from leaders across the agency, including guidance from DCSA Director William K. Lietzau.

DCSA's five-year mission-area strategic goals are:

- Industrial Security: Enable threat reduction and mitigate vulnerabilities to classified and sensitive information and technology in the U.S. industrial base.
- Personnel Security: Identify and mitigate personnel-based threats while enabling customers to onboard talent quickly. This effort is directly tied to the development and deployment of the National Background Investigation Services (NBIS) as part of Trusted Workforce 2.0.

DCSA's 2022-2027 Strategic Plan

Unveiled in April 2022, DCSA's 2022-2027 Strategic Plan supports the agency in meeting the challenges presented by the evolving threat environment. It aligns with broader intelligence and defense strategies and lays the foundation to accommodate DCSA's expanding missions. The Strategic Plan identifies nine goals that will collectively help the agency achieve its mission and vision. These nine goals are divided into two categories: mission goals and enterprise goals. Mission goals will advance mission performance through unity of effort, partnership, and customer experience, and directly align to the four mission areas of the Agency OpModel: Industrial Security, Personnel Security, Counterintelligence & Insider Threat, and Security Training. Enterprise goals cut across the entire agency to empower the workforce by developing and retaining talent to deliver capabilities that support more effective business operations and improve overall mission performance. Read the DCSA 2022-2027 Strategic Plan at: https://www.dcsa.mil/Portals/91/Documents/about/err/DCSA_Strategic_Plan_2022-2027.pdf.



“After much dedicated work, DCSA is implementing its five-year strategy. If done right, this strategy will move DCSA to the next level in its ability to combat threats to our National Security. This is an ‘All Hands on Deck’ effort. The entire DCSA team must be engaged as the strategy impacts every aspect of the Agency from how we do operations in the field, to recruitment and retention, to our culture.”

~ DCSA Deputy Director Daniel Lecce



- **CI and Insider Threat:** Identify, integrate, and share threat information across the enterprise to help drive risk-based, data-driven decisions and actions.

- **Security Training:** Train U.S. Government, industry, and agency personnel to mitigate risk in support of national security.

Breakout Groups: During the offsite, each participant was assigned to one of six breakout groups to address an agency priority needed to achieve the DCSA Strategic Goals. These priority topics included:

- **Common Operating Picture:** Establishing the processes, tools, and staff to centrally receive, track, and disseminate critical DCSA information in a timely and efficient manner.

- **DCSA Culture:** Building a unified DCSA culture that is people and mission-focused, enabling transparency, collaboration, and innovation.

- **Leading in a Hybrid Work Environment:** Providing leadership with tools to lead effectively in a hybrid/virtual environment while meeting mission requirements through connectivity, engagement, and teamwork.

- **Field Structure:** Standing up field and regional headquarters to fully integrate DCSA from operators in the field — across all mission areas — to the headquarters. Further, the field and regional headquarters will ensure the delivery of enabling functions to the field.

- **Recruitment and Retention:** Constructing recruitment and retention strategies to attract and retain talent for our critical national security mission.

- **Cloud Strategy:** Developing and implementing a cloud strategy to ensure DCSA has secure and compliant technological solutions to support present and future operations.

These breakout groups considered solutions and next steps for their respective topics and presented their recommendations to the collective team for consideration, concurrence, and feedback. Now, leadership is focused on putting these recommendations into action and determining tangible activities that will advance these priorities.

WHERE WE GO FROM HERE

Over the next five years, Goal Champions and DCSA leaders will take deliberate and thoughtful action to enhance our agency’s culture, mission, and the services the agency provides. DCSA leadership will keep open and clear communication with the entire DCSA team to ensure transparency and leverage the collective insight and expertise of our dedicated workforce.

NCCS DELIVERS CENTRALIZED REPOSITORY, AUTOMATES DD FORM 254 PROCESS

By Britny Paynter
Industrial Security

Submission of the DD Form 254 (DoD Contract Security Classification Specification), historically, was a manual, paper-driven process in providing the security requirements and classification guidance to contractors and subcontractors necessary to perform on a classified contract. Prior to 2016, no centralized capability existed for the DD Form 254 for the DOD.

The National Industrial Security Program (NISP) Contracts Classification System (NCCS) is an information system designed to deliver a centralized repository for the collection of classified contract security requirements and supporting data while automating the DD Form 254 processes and workflows across the enterprise. The legacy NCCS application, established in 2016 and hosted by the Defense Logistics Agency (DLA), improved the process by providing the community an automated solution and centralized repository. This system was operational from 2016 to 2021 to meet the requirements outlined in Federal Acquisition Regulation (FAR) 4.403 and FAR 4.402.

Despite initial success, the legacy NCCS system faced some challenges which prevented the community from fully realizing its intended capabilities. In addition, the Defense Counterintelligence and Security Agency (DCSA) wanted to incorporate a new capability that allowed users to track and have oversight into Prime, Subcontractor, and Tiered Subcontractor DD Form 254s. These updates would result in development and creation of NCCS 2.0.

On October 1, 2021, the DCSA assumed operational control and development responsibility for NCCS from the DLA, and NCCS 2.0 underwent rapid development to address issues identified by the stakeholder community. The requirements used in development came from both industry and government

stakeholders. Beginning in March, the application went through three rounds of user testing and one round of government acceptance testing.

On June 6, 2022, NCCS 2.0 Minimum Viable Product (MVP) was developed and deployed. DCSA initiated a soft launch with an incremental onboarding approach in coordination with the Military Departments. Additionally, a recent re-write of FAR 4.402 now mandates the use of the NCCS to complete the DD Form 254. Prior to this mandate, submission of 254s didn't necessarily have to be done in NCCS.

The goals of NCCS 2.0 are:

1. To provide a centralized DD Form 254 repository for tracking and oversight.
2. To improve collaboration between the security and acquisition communities.
3. To improve security controls and quality of data contained in the DD Form 254.
4. To improve the contract award process and the NISP Facility Clearance (FCL) and Foreign Ownership Control or Influence (FOCI) oversight missions.
5. To improve transparency of DD Form 254 status and contract security classification specification changes.

DCSA is currently onboarding Government Users in a multiphase approach. Industry user testing and onboarding will begin in November 2022.

For more information, please visit: <https://www.dcsa.mil/is/nccs/>.

For questions, please contact the NCCS team at: dcsa.quantico.hq.mbx.nccs-support@mail.mil.

DCSA BEHAVIORAL SCIENCE BRANCH EFFECTIVELY DESTIGMATIZING MENTAL HEALTH COUNSELING, TREATMENT

[Editor's Note: October is National Depression and Health Screening Month, comprising Mental Illness Awareness Week, Oct. 2-8; National Depression Screening Day, Oct. 6; and World Mental Health Day, Oct. 10. It's a time to reflect on mental health, an important part of our overall health — so take care of yourself.]

By John Joyce

Office of Communications and Congressional Affairs

A new specialty adjudicative branch of the DCSA Consolidated Adjudications Service (CAS) focusing rather behavioral science is expediting security clearance adjudications, as the agency continues its campaign to destigmatize mental health counseling and treatment in relation to the adjudication of national security clearances.

The new Behavioral Science branch — featuring specialists, including eight adjudicators skilled in considering psychological related issues — was a topic of a discussion at a recent Intelligence and National Security Alliance (INSA) webinar, entitled, 'Fact and Fiction: Intelligence and National Security Careers, Mental Health and Clearances.'

"We have adjudicators who provide the actual national security recommendation," said Dr. Michael Priester, DCSA CAS chief psychologist, regarding the branch, which serves as the interface between mental health issues and the adjudication of security clearances. "It's very exciting to have a branch that integrates psychologists and adjudicators to handle sensitive and complex cases."

The Behavioral Science branch adjudicators — expert in either military, business, science or psychological matters — review cases that primarily involve 'Adjudicative Guideline I: Psychological Issues' and co-occurring 'Guideline G: Alcohol Consumption' as well as 'Guideline H: Drug involvement and Substance Misuse matters.

In addition to the INSA dialogue, during a webinar sponsored by the Center for Development of Security Excellence (CDSE) entitled, 'Mental Health and Your Security Clearance Eligibility' held in January,

Priester emphasized the impact of DOD's Trusted Workforce and Continuous Vetting capabilities. These two programs enable early intervention where psychological issues may be present in order to ensure the individual receives appropriate treatment before it mushrooms into bigger problems later and becomes a potential cognizant security concern.

"Mental health stigma persists despite significant efforts to assure that cleared individuals and candidates seeking mental health care itself is seen as favorable — not derogatory — during the vetting process," said Marianna Martineau, Principal Deputy Assistant Director, CAS. "There have been many initiatives supported by DOD to encourage personnel to seek mental health care whenever needed ."

Moreover, the DCSA CAS actively partners with military commands, cleared federal agencies and civilian contractors in an ongoing and collaborative destigmatization campaign focused on busting myths regarding mental health care and treatment.

"The myth busting will be accomplished from basic training or entry to employment and onward," said Martineau. "Commands, agencies and employers need to encourage individuals to seek mental health care whenever needed. We need to equate mental health with physical health and ensure there's no stigmatizing language in policies or in practice that would discourage employees from seeking care or implying that those with mental health conditions are necessarily unfit or untrustworthy."

A detailed analysis of denial and revocation statistics involving psychological conditions clearly demonstrates that a cleared individual is not likely to

lose or fail to gain clearance eligibility after seeking mental health care or experiencing mental health symptoms.

Specifically, DCSA CAS analyzed 5.4 million adjudicative actions from 2012-2020 and discovered that 97,000 cases dealt with psychological-related issues. Of those cases, only 62 were denied or revoked for psychological concerns, which equates to 0.00115% of the total adjudicative actions.

“None of the cases were denied or revoked just for seeking mental health care,” said Dr. Elisabeth Jean-Jacques, DCSA CAS Behavioral Science Branch psychologist. “Most denials or revocations are for multiple adjudicative guidelines, such as personal conduct, financial considerations, alcohol consumption or criminal conduct.”

Other factors — non-adherence to medical recommendations or simply not seeking care in the face of a clear need for mental health support — were considered more concerning issues.

“The data is clear — losing or failing to gain your clearance eligibility for a psychological condition alone is extremely rare, said Priester. “Even in combination with other issues, it is still rare to lose one’s clearance eligibility. Most of the individuals who lost or did not gain eligibility had a variety of issues involved in the case, sometimes as many as six guidelines were cited. Showing poor candor about reporting known psychological conditions raised much more of a security concern, and often led to personal conduct concerns.”

Despite the myth—busting data and the agency’s Mental Health Destigmatization Campaign, studies reveal that a false belief exists among some security managers that seeking mental health treatment could result in security clearance denial or revocation.

“If that positive step to seek mental health counseling or treatment is not taken in relation to some of the cases involving multiple guideline issues, it is probable that the untreated psychological conditions exacerbate other issues or made them worse,” said Priester. “For example, someone with an untreated bi-polar condition may go into a manic episode and engage in excessive spending which could lead to financial concerns because the condition was untreated. Another example would be an individual who is experiencing depression, anxiety or other

(Editor’s Note: Below is an excerpt from an article published by the U.S. Navy about a Sailor who sought mental health treatment for Post-Traumatic Stress Disorder and retained his security clearance.)

Seaman tackled PTSD to make Master Chief

By Mass Communication Specialist 2nd Class William Sykes

U.S. Fleet Cyber Command/U.S. Tenth Fleet Public Affairs

The terrorist attack that struck USS Cole (DDG 67) on the morning of Oct. 12, 2000 left a lasting impact on the crew. They experienced arduous conditions that many Sailors train for, but few will ever see.

Master Chief Information Systems Technician (IT) Amaury Ponciano, from Union City, N.J., was a Seaman at his first command, aboard Cole, during the sneak attack. The crew saved the ship, but lost 17 Sailors including a few who Ponciano considered good friends. The events of that day, left him with Post-traumatic stress disorder (PTSD); but his diagnosis did not prevent him from leading a successful career in the Navy. After 22 years of honorable service, Ponciano was promoted to the Navy’s most senior enlisted rank — master chief petty officer. Only one percent of the force holds the distinction.

He was pinned by his daughter Belen Ponciano, Master Chief Information Systems Technician Dave Berrien and Master Chief Fire Controlman Korey Jones during a ceremony on May 23, 2022.

“[Healing] was difficult because you have to understand yourself and that takes time,” explained Ponciano when talking about his PTSD. “The first years were a struggle. I broke a lot of relationships, with both partners and friends, because my anger would get the best of me. The littlest things would trigger me to no end. Unfortunately I didn’t know how to deal with that.”

In the days following the attack, in the midst of ongoing damage control efforts, maintaining the physical security of the ship and honoring the fallen; Ponciano found inspiration from the Chiefs Mess and the daily raising of the American flag.

“There were things that we young Sailors didn’t understand ... like the Chiefs Mess making us hold colors. It was 120 degrees in Yemen and after all that had happened, it’s the last thing you are thinking about,” said Ponciano. “The way a chief broke it down to me stays with me ‘til this day. He said it was to show them that we haven’t been defeated. That this flag will fly.”

The leadership of USS Cole mandated mental health

common mental health issues but instead of seeking treatment, she or he ‘self-medicates’ by indulging in alcohol and consequently receives a DUI. In both of these cases, if the individual were to seek treatment, that would raise few if any security concerns, but by failing to seek treatment, a much graver security issue would arise.”

DCSA CAS considers their training of adjudicators to destigmatize mental health as vital as the agency applies a “whole person” approach rather than focusing on one incident. “The determination requires team collaboration, supervisory reviews and quality assurance reviews to ensure best informed adjudicative decision has been made,” said Jean-Jacques, adding that subject matter experts — general counsel, insider threat experts as well as psychologists — are on staff for consultation as needed.

Although research shows that stigmas related to mental health treatment have decreased in recent years, the stigma remains a notable challenge — particularly among military members. Many service members do not seek care for mental health symptoms due to reasons such as personal beliefs about self-reliance, concerns about how their supervisors and co-workers may react, and availability of mental health care, according to a RAND study.

“We are further along than we ever have been but we have a big mountain to climb in terms of further destigmatization,” said Priester. “There will always be hesitancy among some people to seek help, particularly in the cleared population who tend to be fairly self-reliant individuals and reluctant to admit they need assistance in any way.”

Early in the CDSE webinar, Martineau, Priester, Jean-Jacques and Jessica Belschner, DCSA Behavioral and Science Branch technical lead, conducted a flash poll. Priester read the true or false statements to the virtual audience regarding psychological conditions and adjudications.

The first question: “There are some psychological conditions that will automatically disqualify you from getting or keeping a security clearance.”

The poll results showed that 75% of the audience believed that was a true statement.

“Hopefully, we can debunk that myth throughout the rest of the presentation — the correct answer is false,” said Priester, emphasizing that there are no psychological conditions that will automatically disqualify you from

resources for the crew once ship returned to the United States a month later. As a Seaman, the mandate provided relief from the stigma Ponciano felt in seeking help. His PTSD diagnosis allowed him to name his trauma and deal with it. Through counseling, he learned to manage his emotions and recognize when he needed to employ coping strategies. He credits the support of his leadership, friends and family and mental health coaching, as contributors to his success.

“I was extremely head strong,” said Ponciano. “I didn’t connect my anger to the PTSD. I remember going to a counselor after being stationed in Bahrain and she would make me tell the story every single time I saw her. I had to learn to express it. To let whatever anger I felt about the story ... to let it out.”

According to multiple military studies, stigma remains a barrier to seeking mental healthcare. Reasons range from concerns regarding how leadership and peers will react, to fear of losing their security clearance. ITs, like Ponciano, manage complex network computer systems to ensure communication across the Fleet to support mission completion. The career field requires Sailors to hold security clearances to access the information and equipment necessary to properly operate the network. Therefore, they undergo multiple background investigations throughout their careers.

“We get the question a lot about PTSD. ‘Is having a diagnosis of PTSD going to impact my clearance ... or ruin my chances at getting a clearance?’” said Dr. Elisabeth Jean-Jacques, staff Psychologist at the Defense Counterintelligence and Security Agency (DCSA) — the Defense organization responsible for adjudicating security clearances. “There is no specific medical diagnosis that is automatically disqualifying.” She also said PTSD is not a reportable condition during the security clearance process.

“If there is a myth out there that, ‘Somehow if I go to behavioral health it will be a career killer’ ... on the contrary, we at adjudications very much see participating in treatment as a favorable thing,” said Dr. Michael Priester, chief psychologist at DCSA. Instead, DCSA adjudicators look for behaviors of concern.

“That can be things like risk for violence, erratic behaviors, or a tendency to not be truthful in a characterological, rather than incident specific, way,” said Priester. “The kinds of things that alleviate concerns with psychological conditions is when someone has sought treatment ... and certainly if they complied with treatment.”

“I am proof. Look at me now. I am a master chief,” said Ponciano.



getting or keeping a security clearance.

The second question: “If a covered individual reports to you that since they last filled out their SF-86, they have been voluntarily hospitalized for psychiatric reasons, this information should be reported to DCSA CAS.”

The poll results showed that 83% of the audience believed that was a true statement. The correct answer is true, said the Behavioral Sciences branch chief, adding that it is a requirement to report voluntary or involuntary inpatient treatment.

Martineau, Priester, Jean-Jacques and Belschner also discussed the risks involved with avoiding mental health care.

The consequences include decreased force readiness — untreated psychological conditions

can increase other physical health issues, negatively impacting a cleared individual’s ability to deploy or perform their job; Increased suicide risks — mental health care is one of the primary protective factors against suicide; and increased security concerns — performing sensitive national security duties while overly burdened by emotional issues could lead to impaired decision making and therefore pose a security risk.

“We can and should shape how the national security workforce perceives mental health care and our commitment to their wellness,” said Martineau.

“Employee wellness is a state of well—being that includes their mental and physical health and that wellness is important to the resiliency of our national security workforce — getting help is

important when it’s needed. We are striving to ensure that our workforce understands that their wellness is important and this requires active engagement at all levels from first line supervisors to security managers to executive leadership. We all must collectively be armed with the information and it’s crucial that support mechanisms are available to employees.”

The DCSA CAS psychologists provide training and education to stakeholders regarding its destigmatization efforts, and has conducted numerous outreach events, to include webinars, presentations, and posting products on the agency external website, https://www.dcsa.mil/mc/pv/dcsa_cas/resources/. For more information or if you have a question, send an email to: dcsa.meade.caf.mbx.comms@mail.mil.

VALUE OF MAKING CONNECTIONS: INDUSTRIAL SECURITY, CI AND BI GROWING STRONGER AS A TEAM

By Field Office Chief Jennifer Norden
Industrial Security

In May and June of this year, the Irving (Texas) Industrial Security Field Office invited DCSA background investigators (BI) to observe security reviews at two large facilities, one in Fort Worth, and one in Oklahoma City. There were several objectives to this collaboration: connect people, connect disciplines, and generate ideas for how to connect this collective expertise for the betterment of security oversight overall. These ride-alongs helped connect names with faces, expanded collegial networks, and provided a better understanding of the geography covered by the individuals who participated in these reviews in Texas and Oklahoma.

The BI special agents each spent a day walking alongside their colleagues, observing one or more of the missions through the lens of an industrial security representative (ISR), information system security professional (ISSP), or counterintelligence special agent (CISA). Both security reviews involved a team of 10 or more DCSA personnel covering various assignments through the course of the week. Each day started with an internal team huddle to coordinate activities and ended with a team meeting to hot wash the results that would be delivered to the cleared contractor's security staff for the daily debrief.

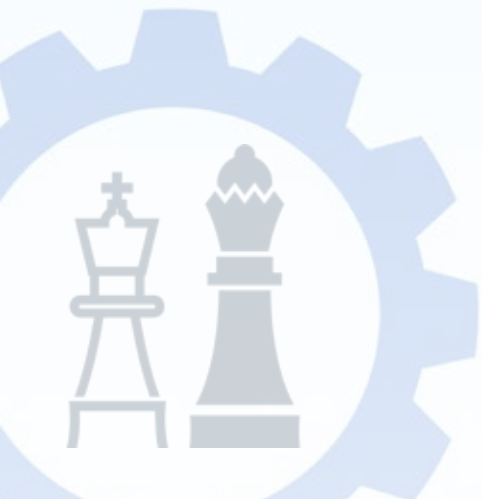
After the morning huddle, the agents set out with one of their colleagues. As expected, the most relatable aspect of the daily work were the interviews the ISRs, ISSPs, and CISAs conducted to evaluate the effectiveness of the contractor's security training program, incorporation of threat products into employees' awareness, and whether employees knew their job-specific duties for handling classified information.

Several BI special agents were taken aback by the random, spontaneous nature of selecting some of the cleared contractors for interviews as the DCSA team walked through cubicles and secure areas, since BI agents generally have specific individuals they meet for subject, supervisor, and coworker interviews.

"Whereas in BI we are looking for testimony about someone else, the ISR interviews seemed more like a 'pop quiz,'" special agent Michael Seufert, BI Fort Worth Field Office, explained. But he recognized there was a reason for this different approach and also found that ISRs and BI agents rely on a similar technique. "What we definitely have in common," he noted, "is the value of open-ended questions and the value of the answers that that elicits."

The ride-alongs also revealed some surprises to those who participated. On the one hand, some presumed that the ISRs would have the most to gain from getting tips and advice on interviewing techniques from the background investigators. While that is absolutely true, Seufert also found that "If all ISRs offered questions in the same manner as the one whom I observed, then ISRs might be able to offer more advice on interview techniques to BI agents as opposed to the other way around which was somewhat surprising."

The other significant take-away is that the ISRs, ISSPs, and CISAs also have a larger learning curve in becoming familiar with the nature of BI work than they or the investigators may have recognized leading into this exchange. "I assumed that everyone else was familiar with the case type names, RSIs (Reimbursable Security Investigations), TESIs (Triggered Enhanced Subject Interviews), etc. This was not necessarily the case," Seufert commented, adding there is "definitely an opening for us to share our processes."



Senior ISR Christopher Flitcraft, IS Irving Field Office, affirmed that the “nuts and bolts” of managing cases, what triggers specific interview types, and how cases are assigned is not something he has direct knowledge of and feels it would “benefit me and others who don’t have BI investigative experience to spend similar time learning what a day-in-the life of a BI special agent is like. I mostly interact with agents when a facility is not being responsive to requests for interviews or records and my assignment to that cleared facility enables me to help resolve those situations.”

As the ISRs, ISSPs, and CISAs conducted their oversight duties, the BI agents observed everything from the basic to the extremely technical. A pretty common and understandable reflection made by agents was that the information systems element was a bit more difficult to digest for those who do not have a background in this field of expertise. But the agents appreciated seeing the wide-range of elements the DCSA team covers and the scope of oversight responsibilities inherent in the security review process.

Connecting dots across disciplines revealed more than the state of the mutual learning curves. As hoped, as the agents and specialists shared what they do, their conversations identified some potential areas to explore for more collaboration in the bigger picture as the integration process continues to evolve.

Seufert noted, “Observing the Counterintelligence special agent (CISA) I think yielded the most opportunities for partnership even though it was the smallest part of my day. I had the opportunity to speak with an Industry CI analyst along with a CISA. Arguably the most rewarding part about this meeting

was being able to describe the BI process to both the CISA and the [Industry] analyst...” Seufert envisions BI, CI, and Industry security personnel collaborating more closely in the future to respond to insider threat indicators.

Special agent Susan Murphy, Oklahoma City BI Field Office, is one of the DCSA investigators who worked for the former Defense Security Service (DSS) before the BI mission was transferred to the Office of Personnel Management in 2005. She suggested restoring a practice from the late 1990s and 2000s in which then-DSS agents would accompany ISRs for new facility orientation meetings to explain the investigative process, recommend some best practices at the outset, and conduct subject interviews with any uncleared key management personnel while onsite.

The agents also similarly commented that walking through the facilities and talking with their IS and CI colleagues gave them more context for what classified work involves. Whether a cleared employee is guarding a perimeter post, developing software for the B-52, or a “custodian” responsible for keeping track of classified materials in a safe, the agents agreed that getting more direct exposure to seeing how cleared employees use their clearances and the types of programs they support can only benefit the agents’ execution of their jobs.

“Having conducted background investigations on [the facility’s] employees for many, many years and visited their site on numerous occasions,” Murphy said, “I felt that I was pretty familiar with their operations but there were still things that I learned that I have taken back with me and that I will use in my job going forward. A couple of examples would

be the specific countries that their personnel are supporting and some of the changes that they are making to their information technology systems which will impact their future security clearance needs. I think that information will allow me to do my job better in the future.”

Reflecting on the team review at a large manufacturing site in Fort Worth, ISR Kamille Staley, who joined DCSA in the Dayton, Ohio resident office just prior to the pandemic and consequently had limited onsite security review experience during her training, explained, “This team review gave me tools to take back to Dayton to conduct security reviews with a new level of confidence in collaborating with others within DCSA. It was great being able to network with all the members of the security review.”

Seufert had a similar comment on the value of the team experience and personal connection. He said, “Overall, I found the experience of observing the industrial security inspection in Fort Worth to be helpful and enlightening. The most obvious benefit of this was simply getting to know individuals from other mission sets within DCSA. We are all under the same umbrella now, and no matter what form any future cooperation takes, it cannot happen without some basic level of interaction and understanding of what we do and how our different mission sets contribute to the overarching goal of national security.”

Murphy, who has experience working under different organizations and has accumulated considerable expertise and perspective over the years, had several particularly salient reflections after observing a large team security review in Oklahoma City. “Working in background investigations is always an interesting job but it also a largely solitary job,” she explained. “It was a joy for me to see the way the industrial security inspection team worked together, collaborated on their final report, and just generally handed taskings off to each other on a real time basis. There was such a smooth flow of communication among the team members that it did make me a little envious.”

Oklahoma City (Midwest City) special agent in Charge Andrew Barnes also joined the IS team for the June security review. He observed the progression of in-briefings by the DCSA team leads, ISR Carlos Chandler and ISSP Keith Williams, with the facility’s security staff, senior management officials, and the regional Defense Contract Management Agency (DCMA) office, and also observed a morning debriefing of findings with the cleared facility. Based on his experience and feedback from the investigators who participated that week, SAC Barnes agreed that this security review ride-along effort should continue whenever workloads and opportunities allow, and that likewise, the ISRs, ISSPs, and CISAs are invited to work with agents to gain better insight into their work.



DCSA CI PUBLISHES CLASSIFIED ASSESSMENT OF THREATS TO CLEARED INDUSTRY

The Defense Counterintelligence Security Agency (DCSA) Office of Counterintelligence (OCI) recently published and released the classified version of the Targeting U.S. Technologies: An Assessment of Threats to Cleared Industry for cleared industry and U.S. Government partners.

The “Trends” is published in response to a Congressional requirement, which directs DCSA to provide classified and unclassified analyses, including annual analysis of suspicious contacts and activities occurring within cleared industry that could adversely affect protection of critical program information.

“The foreign intelligence threat to this nation’s defense industrial base has never been more capable, sophisticated, or complex. To a greater degree than ever before, the importance of technology means that tomorrow’s conflict is taking place today,” said DCSA Director William Lietzau in his introduction published in the Trends. “As adversaries use illicit methods to acquire classified and sensitive information and technologies, they determine the outcome of future conflicts. The time has passed for us to redouble our industrial security efforts. This edition of The Targeting U.S. Technologies: An Assessment of Threats to Cleared Industry reflects the threat picture to inform those efforts.”

Each year DCSA publishes this assessment, focusing on foreign efforts to compromise or exploit cleared personnel, or to obtain unauthorized access to classified information or technologies resident in the U.S. cleared industrial base. DCSA provides a snapshot of its findings on foreign collection attempts and provides analysis that covers the most pervasive foreign collectors targeting the cleared contractor community during the defined fiscal year. This assessment serves to articulate threats to industry and U.S. Government leaders. Due to the COVID-19 pandemic, DCSA has not produced an annual assessment since fiscal year 2020.

Any cleared contractor interested in reviewing this classified assessment can do so by reaching out to their assigned DCSA OCI Special Agent or Industrial Security Representative. The unclassified version is expected to be available before the end of 2022.

SPECIAL AGENTS SUPPORT OPERATION ALLIES WELCOME

Two DCSA Background Investigations employees recently returned from temporary duties that started out supporting the Department of Health and Human Services (HHS) and U.S. Public Health Service Resettlement Program for unaccompanied minors who crossed the United States-Mexico border without family. But due to international events, the duties evolved into supporting Operation Allies Welcome (OAW) and assisting unaccompanied minors and families from Afghanistan.

Special agent Darryl Gray, BI Maryland Field Office, and special Agent Crystal Griffin, BI Colorado Springs Field Office, volunteered for this temporary duty (TDY) due to their aspirations to help others.

“My career and personality has always been focused on providing care, safety and security to the disadvantaged, injured and/or infirmed,” said Gray, who served in the U.S. Air Force and Customs and Border Patrol before joining DCSA. Gray previously supported the southern border mission while working in CBP, as he volunteered for a TDY to Nogales, Ariz., “ensuring the safety and security of persons and cargo at our southern border.”

At the start of their TDYs, both arrived in August 2021, to serve as youth care workers at an Emergency Intake Site (EIS) in Albion, Mich. HHS had established more than a dozen EIS to care for migrant children who crossed the United States-Mexico border unaccompanied by family. The sites served as a temporary shelter until the minors could be placed in the care of a sponsor. The Albion EIS was set up on the campus of a non-profit organization, and unaccompanied minors were housed in ranch-style houses, or cottages, with bedrooms set up for two to three children per room. While at the EIS, the two DCSA employees served as youth care workers,

whose duties included observing and overseeing physical facilities to ensure safety of all children and staff; monitoring direct care and safety of staff and detainees; monitoring maintenance of proper health standards; and liaising with federal staff and agencies to ensure the administration of physical facilities.

Within a month though, the mission changed. “The Southern Border minors were getting reconnected fairly quickly with families, and I was there when the last of the children left,” said Griffin, noting that with the evacuation of Afghanistan, the EIS planned to transition to OAW and begin accepting unaccompanied Afghan minors within a short period of time.

To prepare for the Afghan refugees, the EIS had to be updated to reflect the new mission. “All the signs were in Spanish, which had to be switched to Farsi, Pashto and Dari,” Griffin said. The cottages and mission structure also had to be redone to accommodate the new culture. “We spent 12-16 hours creating Afghan cultural training and teaching it to all Albion EIS staff, organizing new food menus, identifying and engaging points of contact in each appropriate operational area to proactively prepare for our Afghan guests, restructuring an entire cottage with new signs, identified prayer locations facing Mecca and appropriate prayer times, and set up new school and activity schedules,” she said, noting that after obtaining the site commander’s approval, they worked to duplicate the setup in the rest of the cottages.

When arrival of the Afghan families was imminent, Griffin was assigned to duties in the Philadelphia Airport, where she worked with U.S. Customs and Border Patrol and translators to identify unaccompanied minors. “We worked with case managers to conduct interviews and identify any

family members in the United States, or any that may be coming in the future,” she said. Depending on their status, the Afghan refugees were moved to a Safe Haven location or an EIS.

With the arrival of the Afghan refugees, Gray’s mission changed as well. With a background in counterterrorism and counterintelligence from serving in the U.S. Air Force, and with a high degree of training in vetting, he transitioned into the role of safety and security liaison at the EIS site. “My concern was the level of visitors we were getting,” he said, noting that background checks were being done but given his background, he could reach out to the FBI Joint Terrorism Task Force, law enforcement, etc., and also provide briefings on possible threats to increase awareness in the workforce. “My number one goal was safety; how do you keep the children safe? That was the mission. We wanted to protect them from hurting themselves, from hurting each other, while also ensuring the safety of the federal employees.”

By mid-September, Griffin had moved again, this time serving as the site lead for Joint Task Force Liberty under OAW, at Joint Base McGuire-Dix-Lakehurst, N.J., where she managed everything from operations to administration to training. She oversaw a rotating team of 12 to 25 personnel between youth care volunteers, case managers, case management support, cultural advisors working on refugee resettlement as well as assisting needs of the HHS/ORR refugee health support team staff. In that capacity, her minimum 12-hour days usually began at 5 a.m. and often strayed beyond normal operations.

“Aside from all operational activities, our team responded to multiple emergencies while steadily conducting operations and sometimes layered emergencies, which began on my first day on ground where we had a team member sexually assaulted by a contract interpreter,” she said. “So we were responding to the whole operation, while productively dealing with the assault and coordinating with law enforcement and other invested agency partners. The hours were intense but well worth every effort.”

Eventually, Gray also transitioned to Joint Base McGuire-Dix-Lakehurst, working with the case managers in refugee resettlement. After

unaccompanied minors arrived, they were housed in the rooms set aside for them. “The people were well taken care of and referred to as ‘guests’. The commanding general wanted to make them feel comfortable,” he said. “Our team had access to the systems that would facilitate reuniting children with families, and we played an integral role in resettlement and movement.”

Both employees stayed at Joint Base McGuire-Dix-Lakehurst until returning home around the end of February.

In looking back, Gray was proud of the work he accomplished. “It was a hard job, that required flexibility, but it was an interesting mission and rewarding,” he said, noting that no children were injured or abused during his tenure, “except for the children playing soccer in a house and one ended up with a broken toe.”

Gray also noted this TDY supporting OAW closed the loop on a previous mission during his time in the Air Force as a flight medical technician at Rhein-Main Air Base in Germany. “As fortune would have it this mission brought my career full-circle because I was part of the first U.S. military humanitarian aeromedical-evacuation to transport Afghan refugees to the United States during the Soviet-Afghan war,” Gray said.

“This is probably one of the best things I’ve done in my life,” said Griffin, who explained that while in the U.S. Army, she deployed to Iraq. “When you go to war, it’s not a joyful process. Getting to see this side is like coming full circle. I was happy to be that person to welcome the Afghans to the United States and provide them a safe place and process.

“Knowing that we really put in a massive effort is saying it lightly. The level of emergencies we experienced were intense, at best, and we stuck through and responded at every step with great thought and mindfulness about the children involved, first and foremost, and how it affected all other parties as well,” she said. “It was a true serving effort in all aspects; one that we did with great integrity and pride. It was an honor to do so.”

TALK TO THE BOT?

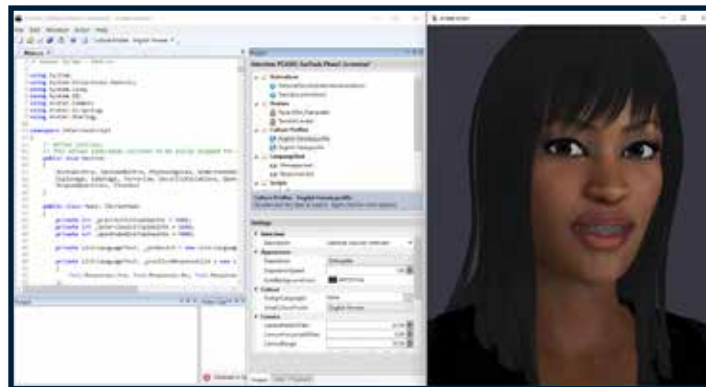
COMPUTER-GENERATED AGENT ASKS QUESTIONS, COLLECTS INFORMATION FOR INVESTIGATIONS



By Dean Pollina, Corey Boswell, Kenneth Ndebele-Duma, Patti Coggins, and Troy Brown
National Center for Credibility Assessment

A research team with the National Center for Credibility Assessment's (NCCA) has, over the last decade, built a software system (project "Avatar") through which an on-screen computer-generated (CG) agent asks questions, and collects useful national security information. In the laboratory, project Avatar was used to conduct polygraph "lie detector" tests. Additionally the research team examined the system's capability to provide automated answers during security interviews similar to those interviewing techniques used by DCSA special agents.

The CG agents within project Avatar are fully-programmable and capable of simulating specific human facial expressions, and are automatically responsive to humans' questions and/or statements. The creation and rendering of these CG characters uses software that was developed in collaboration with Battelle Memorial Institute. It is similar to a modern computer game, in that the CG agents resemble animated feature film characters, but the features can be customized, such as hair, skin, age and eye color. These unique 'agents' are then saved for use in subsequent interviews. A separate interview editor allows the user to generate interview scripts. The software then converts the script into audio files, via a text-to-speech engine, that the user can modify if they want to make the loudness and tone of specific words sound more natural. The audio files then pass through lip-synch algorithms to produce realistic-looking lip movements during the CG interviewer's speech. The CG interviewer is also capable of simulating human facial



expressions either at pre-programmed times or in response to something the interviewee says or does.

How will automated interviewers be used?

The NCCA research team is part of larger, informal group of researchers in the Federal government tasked with developing CG agents in the field of conversational artificial intelligence. As an example, a healthcare bot created by the Centers for Disease Control and Prevention can assess disease symptoms associated with COVID-19. The tool will soon be available on its website. In the future, the NCCA research team will explore the possibility of creating a virtual assistant that could

match agency employees looking for teammates with similar skill sets or experiences. Based on the data that the bot automatically collects, it could also answer questions and supply useful information to the user. As Malcolm Franks points out in *What to Do When Machines Do Everything: 'How to Get Ahead in a World of AI, Algorithms, Bots, and Big Data'*, using AI and machine learning the software can modify itself, learning over time from its past decisions and interactions with humans to improve functional cohesion.

For several years now, the NCCA research team has also been working on using the CG agent as part of an automated national security screening polygraph system. Presently, the polygraph involves a complex clinical process consisting of a human polygraph examiner asking questions that are answered by

the person taking the test. During this process, the examiner continuously records the interviewee's physiological responses. The exam also includes two additional stages: a pretest, prior to the questioning; and, a post-test, after the questioning phase. The NCCA research team is currently studying the possibility of automating the questioning phase, as well as parts of the pretest phase. Whether a polygraph examination can be fully automated is still an open question, due largely to the complex nature of the interactions that can occur between two people during the event. However, preliminary results are encouraging, and reveal several potential benefits to the automation, including: standardization of the polygraph process; and the utilization of longer, more naturalistic types of interview formats.

When will humanoid robots truly seem like humans to us?

Many businesses, as well as DCSA and other Government agencies, are beginning to understand that they have access to far more data than they can possibly comprehend through legacy analytic strategies. In 'The Wiley Handbook of Human Computer Interaction', Kent Norman points out that researchers are now developing new methods to deal with these challenges. In Information Evaluation, Philippe Capet notes that having access to massive amounts of raw data is not particularly useful, unless it leads to better, more informed decisions. Our belief is that new machine learning technologies will be part of the solution to the problem of having too much data.

It appears as though a new AI "boom" is upon us, and this will accelerate the pace of machine learning developments in general and the use of conversational CG agents in particular. There are many signs of its arrival. The best new software gives us a "personalized experience," playing to our unique strengths and avoiding our weaknesses. Specific sub-disciplines within AI that have made major advances recently include automated transcription of audible speech into text; conversion of text to lifelike humanoid speech; photorealistic three-dimensional CG characters; and, natural language translation. These innovations guide our belief that the trend toward using virtual humans in Government and business will continue, and likely increase, in the near-term.

Humans have been creating artificial systems that resemble themselves and can mimic their own behaviors for hundreds of years. Over time, researchers have learned much about what makes human-robot interaction successful. In the social realm, the human's perception that a robot is alive, resembles another human, and is friendly all tend to increase the success of the robot's interaction with humans. In *Living with Robots: Emerging Issues on the Psychological and Social Implications of Robotics*, Richard Pak notes that preliminary research also suggests that people often perceive feminine robot faces as more likable, and findings are similar for human interactions with CG agents of various sorts, to include everything from simple two-dimensional cartoon characters to photorealistic virtual humans. There is also an interesting concept called presence that Kent Norman in 'The Wiley Handbook of Human Computer Interaction', states computer scientists and psychologists define as "the degree of involvement with a game or virtual world." Loosely speaking, we can define it as being immersed in that environment. The degree to which a software environment creates the feeling of presence does seem to be especially important for successful human-computer interactions.

Are there plans for Avatar upgrades?

Beyond using Avatar as a virtual assistant or as part of an automated polygraph, we have accessed the Avatar system in several laboratory studies. The NCCA research team looks forward to receiving input from those within personnel vetting to help determine whether Avatar would be beneficial as part of DCSA's continuous vetting model. It is possible that Avatar could gather information quickly as new security challenges arise, which would enable the DCSA workforce to communicate perceived security gaps and requirements more efficiently; laterally, and across the chain-of-command. In recent years, adversaries have committed various acts of information warfare, including attacks against personal information; industrial espionage; disinformation campaigns; and, cyberattacks notes Daniel Ventre in *Information Warfare*. These threats are not going to go away any time soon, and it is therefore crucial that we define the steps necessary to defuse these threats now.



Defense Counterintelligence and Security Agency

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