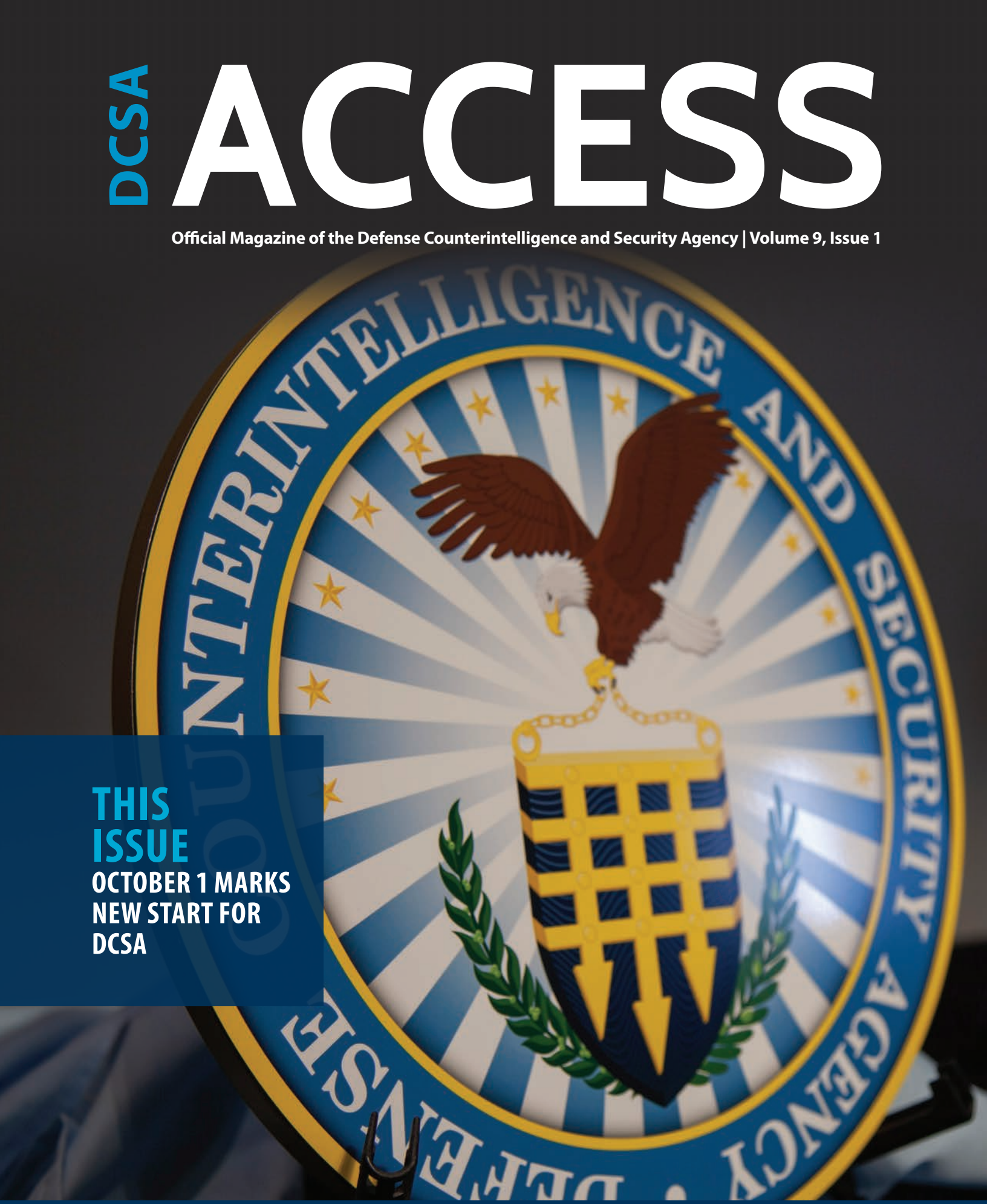
DCSA ACCESS

Official Magazine of the Defense Counterintelligence and Security Agency | Volume 9, Issue 1



THIS ISSUE

OCTOBER 1 MARKS NEW START FOR DCSA

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOL 9 | ISSUE 1

Published by the
Defense Counterintelligence and
Security Agency
Office of Communications and
Congressional Affairs

27130 Telegraph Rd.
Quantico, VA 22134

dcsa.pa@mail.mil
(571) 305-6562

DCSA ACCESS is an authorized agency information publication, published for employees of the Defense Counterintelligence and Security Agency and members of the defense security and intelligence communities.

The views expressed by the authors are not necessarily the official views of, or endorsed by, the U.S. Government, the Department of Defense, or DCSA.

All pictures are DoD photos, unless otherwise identified.

FROM THE DIRECTOR

Welcome to 2020! The New Year is typically a time to look back at what was accomplished in the previous year and forward to the goals and plans for the year ahead. In the case of DCSA, a quick look back is all that's needed to note the successful transfer of the National Background Investigations Bureau and DoD Consolidated Adjudications Facility to DCSA. Overall, I have been pleased with the success of this transfer.

Most importantly, while we worked on the countless tasks associated with the transfer, we continued to execute our mission with no degradation of service. That is a testament to the dedication and commitment of our workforce and stakeholders across the community.

Looking ahead, while we complete the transfer activities, we will focus on organizational transition, and I expect to be in that phase for at least the next year. DCSA is organized around two main mission sets — personnel vetting and critical technology protection — interwoven with and strengthened by counterintelligence and training, and supported by the enabling functions. In this phase, employees and our external stakeholders can expect organizational reviews and realignments as we look to achieve further synergy across our agency.

I know it seems like we have been in one transition or another for the past several years; and we have. But this next transition will develop the foundational elements of Trusted Workforce 2.0, business transformation, and risk-based assessments to a steady operating state. As we move through all this, I will continue to keep you updated.

This edition of the ACCESS highlights some of the accomplishments of the past year, including the formal ceremony marking the stand-up of DCSA and the continued hard work of the DCSA team.

These are exciting times, and I hope that you will be as enthused about the work we are doing as I am.

Charles S. Phalen, Jr.
Acting Director

CONTENTS

OCTOBER 1 MARKS NEW START FOR DCSA

Agency is now largest security organization in federal goverment

Acting Director Charles Phalen (left) rolls the Defense Security Service flag with the help of SSgt. Jenae A. Bellar (right), DoD Consolidated Adjudications Facility, while MSgt. Anthony Cuevas Jr., DoD CAF, holds the flag. (Photos by Marc Pulliam, CDSE)

On October 1, the Defense Counterintelligence and Security Agency became the largest, most significant security organization in the federal government with the successful transfer of the DoD Consolidated Adjudications Facility (DoD CAF) and National Background Investigations Bureau (NBIB) to the Department of Defense. The milestone, two years in the making, was marked by a Casing of the Colors Ceremony and a presentation by Acting Director Charles Phalen to the combined workforce.

On the morning of September 30, the DCSA workforce, along with stakeholders from across the federal government, gathered at the National Museum of the Marine Corps on Quantico, Va., to 'Case the Colors' in a traditional ceremony designed to mark the deactivation of an agency or unit. Each agency has a unique flag referred to as 'Colors' which depict unique aspects of the agency and are displayed to represent the agency. In this case, the Defense Security Service was deactivated and its flag, or colors, furled and secured into a protective sheath and retired symbolizing the formal end of the agency. NBIB was also deactivated while the DoD CAF was merged into DCSA. The new flag of DCSA was unfurled marking the official activation of the agency.

In her opening remarks, Margaret Weichert, Deputy Director for Management, Office of Management and Budget, noted the transfer of NBIB to DCSA was part of a broader management focus for the Executive Branch. She also noted the process began with the FY17 National Defense Authorization Act as an idea to help DoD, when in fact the background investigation mission must be effective and streamlined for all of government.

Weichert urged the combined workforce to continue to improve and said the inventory of investigations decreased at the same time both agencies were focused on the transfer. "We need to be thoughtful and agile in how we bring these missions together," she said. "We must continue to improve."

Weichert briefly touched on future transformation expected under Trusted Workforce 2.0 and how the investigation process is moving to continuous monitoring. "We have to continue to evolve how we look at our workforce," she said.

In closing, Weichert thanked the assembled employees for their hard work in completing the transfer. "As we celebrate, I want to thank you all for going against the naysayers who said it couldn't be done. You have executed a seamless, flawless mission-focused transformation. With quiet competence you have done it and shown that it is simply not true that bureaucracy cannot be changed."

Following Weichert's remarks, the histories of DSS and NBIB were read by Carrie Wibben, former deputy director for Critical Technology Protection, and Christy Wilder, deputy director for Personnel Vetting, respectively. Both noted that the personnel security mission was originally assigned to the Defense Investigative Service in 1972 and

MSgt. Anthony Cuevas Jr. (left), DoD Consolidated Adjudications Facility, straightens the DCSA flag, while SSgt. Jenae A. Bellar, DoD CAF, stands by to assist.

remained in the Department until moving to the Office of Personnel Management in 2005. Now, DCSA is poised to again integrate the personnel security mission into one agency also overseeing the industrial security mission.

Acting Director Charles Phalen and Deputy Under Secretary of Defense for Intelligence Kari Bingen, assisted by Air Force MSgt. Anthony Cuevas, Jr., and Air Force SSgt. Jenae Bellar of the DoD CAF furled the DSS flag and unfurled the new DCSA flag.

Bingen then delivered the keynote address. After welcoming employees, including those viewing remotely, Bingen said she "came on behalf of Secretary of Defense Mark Esper and Under Secretary of Defense for Intelligence Joe Kernan, who believe that 'we have a unique opportunity for unparalleled integration that will

streamline our security clearance program and help maintain our military advantage during a time of unprecedented threats to our people, technology, and industrial base.'"

Bingen added, "We are at a pivotal moment in history — senior statesmen, such as Henry Kissinger, have observed that the United States has not faced a more diverse and complex array of crises since World War II. The technical advantage — that translates to our military advantage — that the United States has maintained for decades is eroding.

"China is playing the long game," she continued, "finding our weak points, using any means possible — legal and illegal — to steal our data, plans, and technologies. People, information, businesses, research institutions… are all targets. We are producing an order of magnitude less STEM graduates than China. Without action, what's in research and development now, what's stolen now… is what our service members will inevitably face on the battlefield.

"You know the challenges facing our Nation. And you chose a career of public service," Bingen said. "You chose to apply your leadership, talent, and ingenuity to strengthening our Nation's security. You ensure that our people, and our most advanced technologies in government, industry, and academia… remain free of foreign, malign influence."

She added, "We owe you an organization that is designed to ensure your efforts are as effective as possible. Congress and the President recognized that when they directed this merger."

Bingen then noted that DCSA shares a 'birthday' with other notable transformative events and organizations. One is the Model T; the iconic car that jump-started the U.S. automotive industry and propelled hundreds of innovations in manufacturing while also driving down the cost. The second is the establishment of NASA, who remains the world's leader in innovative space science and technology and is known for its visionary boldness. And third, Walt Disney World; considered the gold standard for customer service.

Why these examples, "Bold vision, transforming processes at scale, innovation, and customer service… sound familiar? These are the opportunities ahead of DCSA," said Bingen. "May your anniversary brethren offer exemplars for you to pace.

"Through this merger and beyond, background investigations must continue to transform into continuous vetting, maximizing the use of big data analytics and automation, and moving away from arbitrary periods of reinvestigation. Meanwhile, to strengthen industrial security and the protection of our critical technologies, we must continue to partner with industry to move towards a more threat-focused paradigm that reduces risk to both the Department and industry," Bingen continued.

She then cited the accomplishments and initiatives already underway in the personnel vetting and critical technology missions. "As these initiatives evolve," Bingen said, "a unique opportunity emerges with this ongoing merger: a future state where we maintain a holistic picture of risk, integrating both 'risk in person' and 'risk in access,' to protect our people and technologies. The end result being to maintain our Nation's comparative economic and national security advantage."

Bingen offered the following thoughts in closing, "These are unprecedented yet truly exciting times to be in the Security and

Former DCSA Director Dan Payne (left) sits with DCSA senior leadership during the ceremony.

Deputy Under Secretary of Defense for Intelligence Kari Bingen provides remarks at the Changing of the Colors ceremony.

Counterintelligence mission. By bringing together personnel security and industrial security under a single agency, we have created a new strategic asset for the Nation… fit for purpose and fit for our time.

"The challenge is on our collective shoulders," she said, "and it weighs heavily on DCSA. Your mission success is not an option — it is an imperative. I know I speak for Under Secretary Kernan when I say that we have full faith and confidence in you. We know you are up to the challenge, and we are here to support you every step of the way as we move forward.

"NBIB and DSS… you have more than ably carried your "Colors" in your missions throughout these last many years. Be proud of all that you have accomplished, and be bold in the transformation yet to come," she continued.

"As you become DCSA… remember, you are the plank owners. What you do now… the vision you set, the values you uphold, the practices you develop, and the people you foster… This culture, this legacy, will have a profound impact on DCSA for your tenure and for generations to come. We're counting on you."

On October 1, the official start of DCSA, Phalen addressed the combined workforce and offered his thoughts on the occasion. "Yesterday we had a ceremony to "Case the Colors" – formally recognizing the merger of DSS, NBIB, and the DoD CAF into DCSA," he said. In noting the ceremony also deactivated the legacy agencies, Phalen added, "This was more than symbolic, we are a new united workforce, proud of our respective heritage, but committed to our new DCSA."

Phalen said that Day One was just that, ONE DAY. "While day one is just one day, you should all be proud of the work we have done and what has been accomplished during the last year," said Phalen. "But it's the first milestone; there's a lot more to be done to become the complete, fully optimized organization I know we can be."

"Transfer was hard, really hard," Phalen said. The next phase will be Transition and Phalen expects that continue for at least the first year. During the Transition phase, Phalen told the workforce to expect process and organizational review and realignments.

"I expect further synergy between mission sets [personnel vetting and critical technology protection], and just getting to a steady-state," he continued. He also reminded the workforce that no matter where you started, the workforce had been in transition of some kind for the past three years. "Our job is to bring it all together," said Phalen. "I believe this is the right move not only for these missions but also for the whole of government."

After thanking the workforce for their dedication and commitment, Phalen led the agency in reciting the Oath of Office.

SITE VISITS HIGHLIGHT KEY MISSIONS, FUTURE VISION

by Christopher P. Gillis
Office of Communications and Congressional Affairs

Acting Director Charles Phalen, and key senior leadership met with DCSA regional and local workforce during the first round of site visits in Atlanta, Ga., and Huntsville, Ala., in September, 2019. A second site visit to Colorado was postponed due to inclement weather.

The site visits are part of the agency's initiative to enhance employee relations, while working to increase its national recognition with its primary stakeholders – Congressional staff, industry and government stakeholders. The events provided specific sessions designed for and tailored to each audience.

Phalen provided an overview on the direction of the new agency, discussed key topics, multiple transition initiatives and programs, and answered numerous questions during each session. Christy Wilder, deputy director for Personnel Vetting and Ben Richardson, acting director of Industrial Security Integration and Application, also assisted in responding to questions.

Phalen addressed the agency's major initiatives based on two fundamental questions. "Do we have trusted people working in the federal government, and how do we determine that trust?" said Phalen. "And is the work space that industry is working in, and by extension the products that come out of industry, a trusted environment?"

The solution is a combination of programs, the addition of other organizations and the transfer of NBIB, all to be placed under DCSA.

Phalen, Wilder and Richardson emphasized that while we were marching forward to October 1 with the merger of NBIB and DCSA, collectively we have not been waiting on the Executive Order to set plans in place. NBIB and DSS (now DCSA), worked together for over a year, committed to ensuring a smooth transition while minimizing challenges. The legacy agencies focused on critical Day One items to ensure that the combined workforce could continue working uninterrupted.

Phalen discussed his focus and the agency's priorities with future initiatives designed toward an end result with continuous monitoring of our trusted workforce and industry. "There is a natural connection and synergy of these mission sets: Ensuring a trusted workforce and trusted workspaces (real and virtual) that produces trusted work." Phalen said. "While we will continue to perform these fundamental missions, we must also look to the future and how we will ensure synergy occurs."

"Our success in all of these efforts will depend on our partnerships and collaboration with our customers and stakeholders who strengthen our progress and ensure our national security," Phalen said. "I believe this is the right move not only for these missions but also for the whole of government"

TOP: Ben Richardson (left), acting director of Industrial Security Integration and Application, talks about critical technology protection and DCSA initiatives during the panel discussion. **BOTTOM:** Acting Director Charles Phalen (left) and Deputy Director for Personnel Vetting Christy Wilder engage with the audience. (Photos by Christopher P. Gillis, OCCA)

AGENCY BIDS FAREWELL TO DEPUTY DIRECTOR, CRITICAL TECHNOLOGY PROTECTION

In mid-October, DCSA bid farewell to Carrie Wibben, deputy director for Critical Technology Protection, in an informal ceremony held at the headquarters. Acting Director Charles Phalen thanked Wibben for the work she had done at DCSA and said, "Your impact has been tremendous on vetting and critical technology protection. You were always pushing for change and you touched much of what we do here."

In her remarks, Wibben thanked those in the audience who supported and mentored her while at DCSA. "We share a passion for this work," she said. "It's what unites and connects us. It's not just a job; you all take this work personally."

Wibben encouraged DCSA employees to remember why we do what we do. "Remember why this mission matters," she said. "And be prepared to blaze a new trail for DCSA into the future."

Acting Director Charles Phalen (left) presents Carrie Wibben, former deputy director for Critical Technology Protection, with the DCSA Distinguished Service Award.

DCSA EMPLOYEE RECOGNIZED AS DOD OUTSTANDING CIVILIAN EMPLOYEE WITH DISABILITY

by Beth Alber
Office of Communications and Congressional Affairs

Liam O'Sullivan received the 2019 Secretary of Defense Award for the Outstanding Department of Defense Civilian Employee and Service Members with Disabilities during a ceremony in October at the Pentagon.

O'Sullivan, who acts as the Collection Management Officer/Regional Counter-intelligence (CI) Analyst for the Northern Region, supports the agency CI special agents by providing timely, effective analysis. In his collection management officer role, he helps guide the collection process by directing CI special agents to focus on areas of significant interest to national security. Currently O'Sullivan is acting as the CI deputy director for the Northern Region, working to manage and support the region's CI special agents and analysts.

"People might think of counterintelligence analysis as a dry topic, but it's a very rewarding job," O'Sullivan said. "Being able to take the information collected by the field and tie it into the larger national security picture is like having a new puzzle every day. You have all the tools you need to solve it, but you just need to be able to outwit the problem."

O'Sullivan joined the Defense Security Service in 2015, after returning from Afghanistan where he was performing CI duties for a DoD contractor. "I returned to the area where I grew up and decided I wanted to enter the federal workforce," he said. "After some searching, I saw that DSS had a CI analyst position open just up the road from my house, and it was a perfect fit for my skills and interests."

O'Sullivan believes the reason he was nominated for the award was due to his work in CI.

"I was the lead analyst supporting what became a CI investigation," he said. "Along with Frank Bonner, Counterintelligence Special Agent, and Joseph Harne, assistant regional director for the Northern Region, we were able to identify a bad actor and convince our government partners to launch an investigation."

That investigation would lead to a Chinese national being charged with conspiracy to commit export violations, conspiracy to defraud the United States, smuggling, money laundering and making false statements to government officials. He is currently being tried in federal court for these charges.

The Pentagon ceremony recognized 23 government civilians and military service members with disabilities for their outstanding contributions to the DoD mission.

Through his attendance at the ceremony, O'Sullivan realized that DoD considers its disabled employees to be a vital part of the team.

"The experience of being recognized at the Pentagon ceremony was humbling," he said. "To hear about the accomplishments of the other nominees was inspiring. We all had varying degrees of disability, but you wouldn't know it to see the levels of success they had achieved.

"But what really impressed me was the importance placed on the ceremony," he continued. "This was no certificate of appreciation and a handshake, but a full band and the Old Guard, a professional Army singer for the National Anthem, and speeches from the Secretary of Defense, disabled athletes and others, showing just how dedicated the Department of Defense is to supporting their disabled employees."

The Honorable James N. Stewart (left), performing the duties of Under Secretary of Defense for Personnel and Readiness, presents Liam O'Sullivan with his award.

O'Sullivan admits his disability might slow him down at times, but "it just makes me work that much harder to get effective results." But he's quick to note that the agency has programs set up to support those with a disability.

"I would encourage anyone struggling with a disability to reach out to Rosemary Salak, the agency Disability and Reasonable Accommodation Program Manager," he said. "She and her team can work with you to find ways to lessen your disability's impact on your duties."

O'Sullivan also encourages employees to join the agency Diversity and Inclusion Council, which is "a great way to get involved in disability issues if the spirit moves you."

And lastly, "let your supervisor know what's going on if you do have a disability," he said. "My management team at DCSA is 100% behind me and actively works to make sure I'm set up for success."

AGENCY COLLABORATES WITH DAU TO PROTECT CRITICAL TECHNOLOGY

by Betsy Bruinsma
Center for Development of Security Excellence

Traditionally, the acquisition process has been supported by three pillars: cost, schedule, and performance. But now, it is recognized that these pillars must stand on a foundation of strong security to enable the development of uncompromised products and services critical to the nation's defense and economic well-being.

We must prioritize and cultivate a culture of security not only among security professionals but also among acquisition professionals. Just as security professionals will need to become more knowledgeable and informed about the acquisition process, acquisition professionals must also understand the fundamentals of a strong security program.

To this end, the Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) and the Defense Acquisition University (DAU) are collaborating on several fronts to improve the security community's knowledge and understanding of the acquisition process, including supply chain risk management and life cycle logistics, as well as to improve the acquisition community's knowledge and understanding of security fundamentals.

DAU and CDSE are proud to announce the first DAU course available on the Security Training, Education, and Professionalization Portal (STEPP) Learning Management System (LMS). The course, "DoD Supply Chain Fundamentals," is approximately four hours in length and teaches students to identify and recognize key characteristics of Department of Defense supply chain management fundamentals, and effective and efficient supply chains. CDSE will be adding additional DAU courses to STEPP in the future, allowing easier access without the need to obtain a DAU.edu account.

In addition to the DAU courses on STEPP, CDSE is working to make fundamental security courses available on the DAU.edu LMS so acquisition professionals may complete those courses to expand their understanding of security principles. The first course offered on the DAU site will be "Introduction to Risk Management Framework," which is an often requested course by acquisition professionals.

Building on the success of the role-based toolkits CDSE has offered for several years, CDSE and DAU also collaborated to complete two new toolkits. Posted to the CDSE website is an Acquisition Toolkit that provides security professionals with a large number of acquisition resources from DAU. And DAU is adding a Security Resources Toolkit to its site that links to resources developed by CDSE. The Security Resources Toolkit will provide useful resources to acquisition professionals as they expand their understanding of security fundamentals.

As part of their Powerful Examples series, DAU invited former DCSA Deputy Director for Critical Technology Protection Carrie Wibben to participate in an audio interview/podcast and video. Wibben provided a very strong example of the importance of security as a foundation of the acquisition process by discussing a recent Comprehensive Security Review in which the vulnerabilities identified could have been mitigated up front had security considerations been addressed thoroughly during contract award. Both the audio interview and video are available for viewing through both CDSE and DAU.

CDSE and DAU also collaborated to conduct a training needs analysis (TNA) to recommend the appropriate scope and format of training for those Department of Defense assessors who will be responsible for assessing protection of Controlled Unclassified Information on systems. This TNA produced recommendations for the joint development of a multi-phased CUI training program in coordination with Defense Contract Management Agency.

The shared goal of these collaborative efforts is to ensure acquisition and security professionals have access to needed training and other resources to prioritize security as the foundation of the acquisition process. In turn, this will enable the development of uncompromised products and services critical to our nation's defense and economic well-being.

ANNUAL CONFERENCE EMPOWERS COMPANIES TO PROTECT ASSETS MORE EFFECTIVELY

by Will Cooper
Industrial Security Integration and Application

DCSA hosted the 23rd annual Foreign Ownership, Control, or Influence (FOCI) Conference, at the U.S. Patent & Trademark Office in Alexandria, Va., in August 2019. Nearly 500 representatives from industry and government attended, including retired senior military officers, senior government leaders, and chief executive officers. DCSA hosts the conference every year to share best practices and information needed to protect companies in the National Industrial Security Program, that are operating under a FOCI mitigation agreement, and to empower them to protect their assets more effectively.

The conference this year was notable given the changes at DCSA, from the merger with the National Background Investigations Bureau (NBIB) to the appointment of Charles Phalen as acting director. In light of that change, DCSA provided key updates on its evolving mission, explained senior leaders' priorities, and solicited feedback on the FOCI program. Over the course of the day, more than 30 speakers and panelists discussed topics of mutual interest to DCSA and industry.

The conference began with a "general session" for all participants. Fred Gortler, former director of Industrial Security Integration and Application, kicked it off by summarizing some of the year's major initiatives and explaining DCSA's commitment to compressing timelines for agency action. Garry Reid, Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence, surveyed the global threat landscape and reiterated the need to integrate economic, commercial, and defense interests when combating the risks of foreign investment.

Phalen delivered the keynote address, where he noted the increase in the agency's size, explained the paramount importance of a trusted workforce across the government, and emphasized the need to understand the life cycle of what, exactly, is a secret. The first panel of the day then convened as former DCSA Deputy Director for Critical Technology Protection Carrie Wibben and other senior government leaders discussed supply chain risk management issues, including assurance and information sharing, having an awareness campaign within security, and identifying friction points in acquisition.

Heather McMahon, a Senior Director of the President's Intelligence Advisory Report at the Department of Defense, and Dave Stapleton, Office of the Under Secretary of Defense for Acquisition and Sustainment, reviewed the contemporary threat environment as applied to business. They underscored the need for continuous monitoring, pointedly warning industry that every company is susceptible to attempted theft of its intellectual property.

Melissa Hathaway, a FOCI company director, delivered a presentation on cyber risk, highlighting the latency between compromise and detection, and imploring companies to examine not only their appetite for risk, but also their resiliency, in the face of unremitting cyber threats.

> **"DCSA provided key updates on its evolving mission, explained senior leaders' priorities, and solicited feedback on the FOCI program."**

The afternoon portion of the conference consisted of two breakout sessions, with content geared toward either company executives or facility security officers (FSO). The executives' session began with a panel of corporate governance experts from industry offering advice and best practices on how FOCI companies can forge productive relationships with their foreign shareholders, while following the rules of their FOCI mitigation agreements. Next, a panel of government representatives explained how FOCI policy is developed and implemented at the interagency level, illuminating an aspect of the FOCI program that is seldom understood by industry.

The FSO session focused on how NBIB's merger with DCSA will affect industry in its dealings with the new agency. The first panel reviewed, at the strategic level, how the personnel vetting mission will transform DCSA to ensure a trusted workforce across cleared industry. The second panel reviewed changes at the operational level in order to explain how future engagements with DCSA will differ, in that there will be as much focus on personnel as on industrial security. The final speaker of this session, an FSO for a FOCI company, provided attendees with strategies they may leverage to help educate foreign shareholders on FOCI requirements, without compromising effective working relationships.

Initial feedback from participants on the conference has been extremely positive. DCSA will continue to engage with attendees on how to improve the conference before next year, and will persist in underscoring the importance of trust across cleared industry.

INTELLIGENCE OVERSIGHT ENSURES CONDUCT OF CI, INTEL ACTIVITIES WITHIN LEGAL LIMITS

by Beth Alber
DCSA Office of Communications and Congressional Affairs

Intelligence Oversight is the process of ensuring that all intelligence and counterintelligence, activities are conducted in accordance with federal law, Presidential Executive Orders, DoD directives, regulations, policies, standards of conduct, and propriety.

The need for an Intelligence Oversight program within DoD has its roots in activities during the Civil Rights movement and the Vietnam War protests. As protest demonstrations got less peaceful, the military was brought in to restore order. The military units needed intelligence to perform their mission and this led to gathering information on U.S. civilians involved in the demonstrations. As time went by, the collection efforts led to abuse of the Constitutional rights of U.S. citizens. Several Congressional committees established task forces to explore the issue, and in 1976, President Gerald R. Ford signed Executive Order 11905, which placed several controls on intelligence operations. That E.O. evolved and in 1981, President Ronald Reagan signed the current E.O. 12333, which continues to balance intelligence activities with the Constitutional rights of U.S. citizens. DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons" was published in 1982 to codify DoD's responsibilities with respect to E.O. 12333.

The agency Intelligence Oversight program was initially established in 2010 in the Office of the Inspector General (IG) with IG employees conducting required Intelligence Oversight inspections as part of the IG oversight mission. DoD 5240.01M was published in 2017, updating and replacing a majority of content found in DoD 5240.1-R, and contained a provision that agencies conducting intelligence activities appoint an Intelligence Oversight Official. In July 2019, Tim Crawford was hired as the agency's first Senior Intelligence Oversight Official.

Crawford previously worked in Intelligence Oversight with the U.S. Army's Intelligence and Security Command (INSCOM), where he was responsible for approximately 17,000 INSCOM intelligence personnel worldwide, had technical oversight of command investigations in allegations of questionable activities, and conducted Intelligence Oversight inspections of INSCOM elements in Japan, Europe and throughout the United States.

Since coming on board, Crawford said his focus is on the conduct of intelligence and counterintelligence activities within DCSA, and the personnel conducting those activities. "Purpose drives authority," he said. "The reason DCSA personnel collect, maintain, and disseminate U.S. persons' information determines the DoD authorization," noting that collections for security or administrative functions have a different DoD authorization than collections for intelligence purposes.

"All intelligence personnel need to understand their purpose, mission, and authorities for conducting intelligence activities," he continued. "However, while laws and DoD issuances technically allow certain activities, all DCSA personnel should ask themselves – "Can I?, May I? and Should I?"

Crawford went on to explain, "Can I?" refers to the person having the technical training and capability, while "May I?" is the requisite authority and legal approval to conduct the activity, but "Should I?" requires some critical thinking to answer. "A person needs to ask themselves if what they are doing is ethically and morally correct," he said, "and is the chain of command aware of the risks associated with this activity."

In an effort to increase awareness of the program, Crawford has created communications materials, and developed an internal website to act as a one-stop shop for employee's to access directives or publications related to intelligence activities. He also realized the need for cross-talk among the region's counterintelligence deputy directors, who also act as the region intelligence oversight officer, to discuss the DoD Senior Intelligence Oversight Official program and its inspection methodology, identify intelligence oversight concerns, and establish an inspection agenda.

He has completed a rewrite of the agency's Intelligence Oversight Program regulation, and he's revamping the agency's inspection methodology to focus on adherence to DoD issuances, while also reviewing effectiveness. "The combination will help identify what may be hindering an agent's ability to conduct necessary CI activities in support of cleared industry," he said.

Intelligence Oversight training is mandatory for all DoD personnel. With that in mind, Crawford is working with the Center for Development of Security Excellence to revamp the annual training to bring it into compliance with current regulatory guidance. For new employees, he created the "Intelligence Oversight at a Glance" training sheet for use when access to training isn't possible.

"Through a campaign of 'teach, train, mentor,' my goal is to develop, implement and sustain a robust intelligence oversight program across the DCSA enterprise," he said. "Ultimately, I hope this will produce a catalyst of change for personnel to bring intelligence oversight to the forefront of their minds, rather than as an afterthought."

ASK THE LEADERSHIP

A Q&A WITH VALERIE JOHNSON & JACK JIBILIAN

Editor's Note: Each issue of the ACCESS features an interview with a senior leader on their background, mission and program and priorities. The October 1 merger of multiple agencies means a different baseline understanding of key elements of the agency. One such area is Financial Management, where DCSA will maintain its two legacy financial systems: appropriated funding and a working capital fund. In this issue, we talked to Valerie Johnson to explain the appropriated funding side, and Jack Jibilian to explain a working capital fund.

Valerie Johnson is currently the acting deputy chief financial officer of the Financial Management Division. Her federal career began with the Department of the Navy in 1981 where she worked in several positions. Her last position was with the Chief of Naval Operations, Logistics, Depot Maintenance. While with the Navy, Johnson was awarded the Civilian of the Quarter in 1998. In 2002, Johnson joined the Washington Headquarters Service (WHS) Financial Management Office as a budget analyst for the Defense Facilities directorate and ultimately became the WHS Revolving Fund Analyst with the WHS Comptroller office. Johnson joined the Defense Security Service in 2008 as the Chief, Program and Budget in FM. Johnson graduated from Park University with a Bachelor of Science degree in Management. She is a member of the American Society of Military Comptrollers, a Certified Defense Financial Manager, and is DoD Financial Management, Level 3 Certified.

Jack Jibilian is assigned to the Office of the Chief Financial Officer and oversees DCSA's new Working Capital Fund. In this role, he provides management, oversight and analysis of the Working Capital Fund with over $1 billion in annual revenue. Jibilian is responsible for budget formulation, budget execution, and financial reporting, to include the development of annual investigative case pricing, customer billing oversight, and out-year financial projections. Before joining NBIB, Jibilian served a 26-year career with the U.S. Air Force, receiving his commission through the Reserve Officer Training Corps at the Pennsylvania State University. Following his retirement from the Air Force in 2011 as the Director of Engineering for the Air Force Battle Management Program Executive Office, he joined the Air Force's Electronic Systems Command as the Chief for Enterprise Engineering where he directed the development of the U.S. Air Force's next-generation information technology security infrastructure. In 2012, Jibilian joined OPM's Federal Investigative Services as the Chief for Division Support, and in 2015 was selected as Executive Program Director for Finance and Performance for NBIB.

Q Tell me a little bit about your background? What was your position in the legacy organization and what is your position in DCSA?

A Johnson: I have been working with the federal government in the Department of Defense for 38 years to include 35 of those years in Financial Management where I have worked from the bottom up on all phases of the Planning, Programming, Budgeting and Execution (PPBE) process. These years of service have provided me with a wealth of knowledge and broad perspective on how the DoD financial management process operates.

In the legacy Defense Security Service, I was the Chief, Program and Budget in the Financial Management division responsible for leading the budget formulation team on the development and submission of the agency budget justification materials and execution of the agency budget. In my current position, I am the Chief, General Fund branch and acting deputy chief financial officer responsible for leading the team across all aspects of the financial management day-to-day operations.

Jibilian: After a very rewarding career in the Air Force, both on active duty as well as a civilian, I joined the Federal Investigative Service (FIS) seven years ago and continued to contribute to our country's defense. I was originally hired to do performance,

analytics and enterprise reporting as well as general program support such as human resources and workflow management. I was asked to lead FIS', and soon NBIB's performance and finance activities about four years ago, running the daily operations of the NBIB portion of OPM's Revolving Fund. Before the DCSA merger, I ran all financial operations for NBIB and its performance, enterprise reporting and analytics capabilities.

Under NBIB, besides financial operations, analytics was a big part of my office's responsibilities. Our goal was to provide leadership with analyses so they can make the most effective, informed decisions for the background investigation enterprise across the federal government. This included business intelligence, predictive analysis, and effectiveness of our business processes. One example was our weekly key performance indicators, or KPIs. This report gave OPM, DoD, DNI, and OMB leadership insight into how well NBIB operations were delivering background investigation services to our federal customers in a timely and high quality manner.

We also worked as a performance and financial team to employ predictive analysis to build our cost model to develop future case prices. To effectively support our customers, we are setting prices 15 months in advance of issuing them — which is no easy task. We don't want to underprice the work but we also don't want to overprice it. It's a challenging process.

Q Bringing together two disparate financial operating systems from the legacy organizations presented many challenges. Can you discuss some of them and how you and your staffs overcame them?

A Johnson: To clarify, the working capital fund is not considered a system, but a source for financing for the DCSA background investigation mission. That said, there were plenty of challenges. With limited resources, the DCSA Financial Management team was given the responsibility to establish a Working Capital Fund infrastructure in support of the transfer of the background investigation mission from OPM. The goal was to ensure that operations remained solvent at all times and to operate efficiently keeping the cost of investigations stable.

With limited resources, we were responsible for the transfer of 2,500 plus legacy NBIB employees into the Defense Travel System (DTS). This included issuing government travel charge cards accordingly. Another challenge was the changing the culture of the financial management landscape to include the Working Capital Fund. We are currently establishing process and procedures for use across the agency on the use of the Working Capital Fund vice the general fund. And we're doing all of this to include merging a financial management team that is not co-located.

I think the Financial Team has been able to overcome these challenges by having a dedicated and knowledgeable workforce who does not believe in mission failure. We have had to roll up our sleeves to take on duties and responsibilities that were outside of our normal scope of duties and think outside the "box." In addition, we made field trips to meet with various defense agencies to gain knowledge and expertise on the Working Capital Fund.

Jibilian: It's important to remember, the two legacy financial systems; the appropriated funds that legacy DSS relied on and the Working Capital Fund managed by legacy NBIB will remain separate and that's a legal requirement. We cannot mix the two types of funds. But many of the financial processes and reporting responsibilities are very similar within the DoD, so we want to ensure we use similar processes when able.

That said, NBIB was part of a Revolving Fund administered by the Office of Personnel Management. Moving into a Working Capital Fund administered by DoD presented its own set of challenges. There were multiple agencies involved in moving the funds to include the OSD Comptroller, the Department of the Treasury and the Office of Management and Budget. DoD has different requirements for how a Working Capital Fund works from that of OPM. For example, we needed to execute new agreements with each of our over 100 federal customers who use our investigative services. We had an aggressive education process to help them understand what they needed to do and how things would be different in DCSA. We pay many records providers for information we include in our background investigations, so we had to ensure we could smoothly continue these agreements. In addition, we had to ensure we continued to provide the field investigation workforce with such activities as travel and other financial support. Although it simply appeared like we should just open a new checking account at a new bank and start business, but it was much more very complex. Not the very least was to ensure our entire workforce was seamlessly paid during the transition. The DCSA Financial Management and Human Capital Management Offices went above and beyond to make sure that happened.

Q Many in the legacy DSS have no experience with a Working Capital Fund. Can you explain what it is, how it works and how it is different from appropriated funds?

A Jibilian: In simple terms, the Working Capital Fund is not tied to a specific fiscal year – unlike appropriated funds Working Capital funds don't expire on September 30. It also must operate as a full cost recovery program; in other words, we execute our mission with the funding we charge our customers to deliver the service. It's all based on the cost of doing business; we don't get any additional pot of money from Congress to operate. The fund must be self-sustaining and is based on established service prices, taking into account the costs associated with running the program. The prices paid by the customer for our services must cover all costs. This includes direct operations costs, such as labor, travel, training, investigative contracts and indirect costs, such as facilities operation and maintenance. It also includes hardware costs, such as acquisition and repair of

equipment needed to support warehouse operations. As I mentioned before, we set our costs 15 months ahead of implementation with the rates locked throughout the fiscal year (except under extraordinary circumstances).

The balance in the Working Capital Fund will have gains or losses within each fiscal year. If we have gains, we may return them to customers by setting lower rates, and we can also establish higher rates to recover losses. Just like an individual checking account, a Working Capital Fund must maintain a positive cash balance at all times.

Johnson: The appropriated funds are also known as general funds and are direct appropriations from Congress as specified in the yearly Presidential Budget enacted into law such as through the National Defense Authorization Act. This includes various appropriations: Operations and Maintenance (1 Year), Research Development, Test and Evaluation (2 Years), and Procurement Funding (3 Years), and Military Construction (5 Years). The appropriated funds must be used for the authorized purpose, amount, and time period as specified.

Q How have you worked to integrate the FM staffs given the two financial systems?

A Johnson: The Chief Financial Officer and leadership teams from the legacy organizations meet on a weekly basis to discuss and establish relationships essential to execute the Financial Management mission. In addition, several working groups have been established to develop end-to-end business processes as it relates to day-to-day financial management operations.

Jibilian: As a hard working team. Under the expertise of DCSA's Chief Financial Officer and staff, and the former NBIB staff, we identified the highest priority challenges and tackled them first. The teams then went right to the critical details, and worked as a team to address them. The Working Capital Fund is very new to DCSA, and is very different than appropriated funds management. But it is also very similar. We captured the differences and worked to establish process and procedures within DCSA for them. We then built upon the similarities of the two funds, and collaborated to include the Working Capital Fund in the very robust financial process and procedures that already existed in DCSA.

Q What do you see as the biggest success in the transfer of the financial management area?

A Johnson: The biggest success was standing up of the Working Capital Fund infrastructure in a short period of time with limited staff, while continuing day-to-day operations with minimal disruption to successfully execute 100% of the agency funding at year-end.

Jibilian: There are quite a few to say the least, but three come to mind right away. First, the successful payment of all DCSA's new employees. There are a lot of unsung heroes who made that happen. Second, was the successful transfer of OPM's Revolving Fund balance into DCSA's Working Capital Fund. Not only did we create a brand new Working Capital Fund in DoD, but the team worked extremely hard with the Department of Treasury, OMB, OPM, and OSD to successfully transfer just short of $1 billion the first week of October. Through this effort, we ensured our program has the needed resources right out the gate to continue and even improve its critical mission for our federal wide customers. Third, was the onboarding of our 100 plus customers. We have a ways to go to complete this work, but the hard work to build a process, the technical solutions to support that process, and the communications and outreach to our customers to ensure we effectively served our customers on Day One, and received payment for it, was simply an outstanding effort.

Q What do you see as the biggest challenges still facing DCSA from a financial perspective?

A Johnson: The biggest challenge I see is hiring the required Financial Management staff with Working Capital Fund and General Fund knowledge and experience to meet the demands of the evolving agency mission. DCSA must continue to build solid requirements and strong budget justification materials in order to protect limited resources across the Future Years Defense Program from congressional marks, department-wide reductions, etc. In addition to protecting resources, DCSA must be able to provide performance evaluations that will assess the effectiveness of activities, initiatives and investments as pertains to agency funding.

Jibilian: Again there are a few, but to me right now it is fine-tuning the processes to support our Working Capital Fund team here in DCSA effectively. We did a lot to prepare for Day One, but there is still a lot to do. This includes the ongoing work preparations from last fiscal year, but also tackling the challenges we didn't expect. Some examples include travel, and developing the detailed agreements and then paying our numerous service providers across the country smoothly and effectively.

Also, working the overall execution of the Working Capital Fund, in conjunction with the general fund, is an area we definitely need to get our arms around. For example, getting guidance out to our workforce on what and how the working capital fund can pay will be very important. The Chief Financial Officer is leading that effort now.

Lastly, managing our costs so we can deliver the best products and services for the dollar to our federal agency customers. As we expand our services to continuous vetting, and new standards such as Trusted Workforce 2.0 roll out, we will be teaming closely with the Personnel Vetting Deputy Director and other DCSA senior leadership to take a hard look at our current costs and determine how we need to trim, or increase, our capabilities to meet the changing needs our mission supports in the defense of our nation.

MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP MEETS TO STANDARDIZE SECURITY

Editor's Note: The following reflects the thoughts and opinions of the author on her participation in the 34th Multinational Industrial Security Working Group Plenary

by Dr. Kim Colon
Industrial Security Integration and Application

The 34th Multinational Industrial Security Working Group plenary was held in Split, Croatia, in September. This annual event, including 34 nations, was hosted for the first time by the director of the Office of the National Security Council in Split. Croatia, which achieved independence in 1990, has been a fully-fledged member of NATO since 2009.

For over 30 years, the MISWG has been committed to the standardization of security procedures related to Foreign Ownership, Control or Influence (FOCI), visit requests, hand carriage plans, program/project security instructions, etc. These procedures are available to NATO and other select countries which allow increased efficiencies for all. Bringing nations together is no small feat…this one body of disparate nations unifying in the interest of national security is a testament of what can be accomplished together.

Additionally, the global landscape has evolved since the MISWG was established in 1985 as a non-governmental structure. Thus, the criticality in ensuring information security amongst nations cannot be overstated.

On the first day, pre-MISWG Ad Hoc Working Group (AHWG) meetings took place. These working groups consist of cyber, transportation, facility security clearance /personnel security clearance, and FOCI. As a part of the first day of events, guest speakers from industry explained their transportation plan process. The next few days were filled with breakout sessions on the MISWG vision, mission, and goals; national reports on strategy, FOCI, and cyber; scope of operations review; document governance and next steps; as well as many other items. On the final day, the first industry panel of companies from Germany, the United Kingdom and the United States was held, followed by a discussion on how MISWG and industry could work together. We then had a presentation by the 2020 host nation – Latvia! The MISWG chair preceded in the handover of the MISWG bell.

As this was my inaugural MISWG, it was an honor and a privilege to be part of the U.S. delegation, which also included Mark Smith, Office of the Under Secretary of Defense for Policy/Defense Transportation Security Agency, and Jamie Long, DCSA International Programs, who both co-chair the Transportation Plans working group, along with Mauro Squitieri from Italy.

CONSOLIDATED, CONSISTENT OVERSIGHT APPLIES TO ACCESS ELSEWHERE COMPANIES

by Jerilynn Hunley
NAESOC

Of the over 12,000 facilities in the National Industrial Security Program (NISP), approximately 8,000 are non-possessors of classified information, or "access-elsewhere" companies. The majority of these cleared companies provide their personnel as consultants, subject matter experts, or other service suppliers who may not work on critical technologies or components. Yet, all NISP companies require full National Industrial Security Program Operating Manual compliance and oversight. With the implementation of Risk-based Industrial Security Oversight (RISO), these access-elsewhere companies were often at the bottom of the prioritization list. Realizing these companies received a lower prioritization but still played a large role with other industry partners, whether providing expertise or playing a role in their supply chain, DCSA needed to develop a strategy that engaged these companies at a much higher pace without overloading the already stretched field resources. The result is the creation of the National Access Elsewhere Security Oversight Center (NAESOC), which is a centralized field office providing consolidated, consistent oversight and security management over select access elsewhere companies across the NISP.

The NAESOC approach is designed to address non-possessor threats and vulnerabilities by increasing targeted engagements and conducting active monitoring, risk identification, and proactive outreach and education. The NAESOC's assigned staff is augmented with expertise from Counterintelligence, Personnel Security, and the Center for Development of Security Excellence (CDSE).

Since the first assignment of companies into the NAESOC in late July 2019 (during the pilot), the team has been working to reach out to all the NAESOC companies. They found some have not stayed up-to-date with current DCSA requirements and don't have National Industrial Security System accounts. The team has approved 277 NISS accounts since July (and that's not including the accounts that were rejected). The first outreach to these facilities was through a welcome email pointing to the NAESOC website, frequently-asked-questions page, and providing contact information. Since then, nearly 2,000 companies have been transferred to the NAESOC, and the emails and phone calls have been flowing.

It has become apparent that contacting all NISP facilities, even those not working on critical technologies, is extremely important. Not only have companies reached out to the NAESOC to report changed conditions (143 within a 45 day priod), but the NAESOC has also discovered 39 vulnerabilities through the conduct of 32 continuous monitoring actions. Two of the vulnerabilities were critical, to include one submitted for invalidation because the senior management official did not hold a personnel clearance, and had not submitted his Electronic Questionnaires for Investigations Processing (e-QIP) since becoming president last year. Several other major incidents were reported to us through the NAESOC: one cyber intrusion, and one scenario where a commercial carrier delivering classified weapons prevented unauthorized disclosure to an uncleared person by staying overnight in his truck with the classified materials. Other than security incidents, the NAESOC has found that contacting these access-elsewhere companies has already resulted in the administrative termination of 18 facility clearances. The facilities no longer had classified contracts, but never informed DSCA.

Thanks to the NAESOC team members, we have been discovering and uncovering issues at many access-elsewhere companies, and opening the doors of communication.

ANSWERING QUESTIONS FROM INDUSTRY:

Will additional Category E facilities be transferred to the NAESOC?
Short answer, "Yes." The NAESOC was designed to provide oversight for more than 5,000 Category E facilities in order to allow the field to focus its efforts on providing more effective oversight for possessing facilities. Additional facilities will be transferred to the NAESOC, but those transfers are not planned for several months and will be managed by NAESOC to reduce any friction. In all cases, assignment to the NAESOC is sponsored by current field offices and only happens after the ISR confirms the company has established their security program.

How can I learn more about the NAESOC?
There are several ways to be aware of the most recent status of the NAESOC and industry participation. There is a NAESOC webpage at (https://www.dcsa.mil/mc/ctp/naesoc/) that includes a list of frequently asked questions and a Slick Sheet explaining NAESOC execution and capabilities. Facilities transferred to the NAESOC receive a direct welcome email from the NAESOC team, and will have their field office reflected as "NAESOC" within NISS. Assigned facilities can connect with the NAESOC team either through NISS messaging, by calling the NAESOC Knowledge Center at 1-888-282-7682 (option 7), or by emailing the NAESOC at dcsa.naesoc.generalmailbox@mail.mil.

The participants of the 4th annual Irreverent Warriors Silkies Hike walk through downtown Memphis.

CI SPECIAL AGENT PARTICIPATES IN EVENT, HOPES TO INCREASE AWARENESS OF VETERAN SUICIDES

By Eric Wallace
Huntsville Field Office

Editor's Note: The following reflects the thoughts and opinions of the author on his participation in the 4th annual Irreverent Warriors Silkies Hike - Memphis.

In September 2019, I participated in the 4th Annual Irreverent Warriors Silkies Hike - Memphis. Irreverent Warriors is a nonprofit organization dedicated to bringing veterans together to improve mental health and prevent veteran suicide. Irreverent Warriors hosts numerous events around the country throughout the year.

Silkies Hikes are open to veterans, active duty military, National Guard, and reservists. Participants hike 22 kilometers, carrying 22 kilograms in a ruck sack, while wearing silkies shorts and combat boots. The number '22' represents the 22 suicides committed by active duty and veterans every day. The Irreverent Warriors Silkies Hikes are designed to PREVENT veteran suicide by bringing veterans together using humor and camaraderie to heal the mental wounds of war.

The Memphis hike was an amazing event. There were hikers in there early 20's still on active duty and Vietnam veterans in their late 60's. Every service was represented. People carried flags and guidons from the Army, Air Force, Marine Corps, Navy, and Coast Guard. There was even a Crayola flag carried by several Marines.

I enlisted in the Army in 1999 as a counterintelligence agent when I was 20 years old. I served on active duty until December 2004, and then I returned to the Army as a civilian counterintelligence agent and stayed until early 2010. I deployed to Iraq as the special agent in charge of a counterintelligence detachment in 2008 and 2009.

Participating in the Silkies Hike was one of the most physically and mentally challenging activities I have undertaken in a long time. I trained for three months to prepare for the hike.

During the hikes, boots and carrying the extra weight are optional, but I ended up hiking with 22 kg and wearing running shoes.

During the hike I met services members and veterans from all the services and different ages. They were all just like me. We all had very similar life stories and very similar struggles; we were all a little broken. This event gave me the chance to connect with people who were struggling with the same issues as me. It let me know that I was not alone in my struggles to sleep or to find people I could talk to about things that were bothering me in a way that was meaningful to me. The physical and mental aspects of hiking 22 kilometers and the rewarding feeling of finishing were also healing.

I strongly encourage any veteran who is struggling, looking to connect with other veterans, who want to help and support other veterans, or who just want to let their hair down a bit and have a good time, consider participating in an Irreverent Warriors Silkies Hike. Irreverent Warriors is very active on their Facebook site, or you can find the schedule of upcoming hikes on their website, https://www.irreverentwarriors.com/. As the Irreverent Warriors site states: "The connections and bonds made at our events allow veterans to create their own support network solving the most crucial issue contributing to veteran suicide; isolation. Eliminate isolation, and we'll eliminate suicide."

DCSA ACCESS

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY | WWW.DCSA.MIL