DSS ACCESS

Official Magazine of the Defense Security Service | **Volume 8, Issue 2**

THIS ISSUE

DSS EXECUTES FIRST OTHER TRANSACTION AGREEMENT FOR CUTTING-EDGE TECHNOLOGY

VOL 8 | ISSUE 2

Published by the
Defense Security Service
Public Affairs Office

27130 Telegraph Rd.
Quantico, VA 22134

dsspa@mail.mil
(571) 305-6751/6752

DSS LEADERSHIP

Director | Dan Payne

Executive Director | Troy Littles

Chief, Public Affairs | Cindy McGovern

Editor | Elizabeth Alber

Layout and Graphics | Stephanie Crisalli

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

FROM THE DIRECTOR

On April 24, 2019, the President signed Executive Order 13869, *Transferring Responsibility for Background Investigations to the Department of Defense*. This E.O. sets in motion activities to transfer the National Background Investigations Bureau from the Office of Personnel Management to the Department of Defense, to be integrated with DSS by October 1, 2019. The E.O. gives initial direction to the Director of OPM and the Secretary of Defense for the transition and establishes overarching time frames for this organizational shift.

As I have shared before, the DSS and NBIB transition teams have been working in concert to prepare for the transfer of NBIB's mission, personnel, resources and assets to the Department in a transparent and seamless manner, while we continue to execute our core mission areas:

- Secure the cleared national industrial base against attack and compromise
- Conduct security and suitability background investigations and adjudications
- Serve as the premier provider of security education, training, certification, and professionalization for the Federal Government, industry, and allied partners
- Identify and neutralize foreign intelligence threats to the Federal Government's trusted workforce and critical technologies

We are committed to an open, transparent transition process and will keep you informed as new information becomes available and key decision points are resolved. For our cleared industry partners, your industrial security representative remains your primary point of contact for the latest information.

A strong NBIB-DSS team, merging into the Defense Counterintelligence and Security Agency, is our best combination for success for our many partners and stakeholders. Together, we will seek continuous improvements to processes and policies, and implement initiatives to meet the needs of our stakeholders more effectively. We have an unprecedented opportunity to modernize and reform the vetting enterprise for personnel and contractors across the Federal Government, and ultimately to better secure our nation's technological, economic, and military advantage. Although DSS and NBIB will have a different name and a new structure in the future, we both have a single focus: to allow trusted people and technology in, while keeping adversaries out.

I thank all of you for your support as we begin this transformation.

Dan Payne
Director

CONTENTS

COVER STORY

INSIDE

ASK THE LEADERSHIP

AROUND THE REGIONS

COVER STORY

DSS EXECUTES FIRST OTHER TRANSACTION AGREEMENT FOR CUTTING-EDGE TECHNOLOGY

by Stephen Heath
Office of Acquisitions

To solicit cutting-edge technologies and meet the changing needs of its customers, the Office of Acquisitions is using its first Other Transaction Agreement (OTA) to enhance mission effectiveness. This OTA will prototype the use of publicly available electronic information in the continuous vetting mission, and is one piece of DSS' overall mission to transform the security clearance background investigation (BI) process. In addition to its initial award, Acquisitions expects to award up to five additional OTAs this year as part of the agency's BI transformation efforts.

Using the OT authority for prototypes granted to the Department of Defense provides an acquisition method designed to streamline acquisitions for prototypes of items or processes. The OT acquisition process allows DSS to reach out to non-traditional government contractors to seek new ideas, technologies and energy.

The OT acquisition process allows DSS to reach out to non-traditional government contractors to seek new ideas, technologies and energy.

It also allows DSS to use commercial best practices, instead of being restricted to the rigorous requirements of the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS), while maintaining a competitive process overseen by technical subject matter experts, acquisition/contracting, auditing, and legal professionals.

The traditional FAR- and the DFARS-based acquisition strategy is designed to procure what the government needs at a fair and reasonable price. But it sometimes curtails the ability to reach technology companies who are not inclined to do business with the government for whatever reason, thereby impeding innovation.

The FAR and DFARS process is initiated when a need is recognized and the requirement is well defined. Then the Acquisition Team develops a Statement of Work (SOW), a Performance Work Statement (PWS) or a Statement of Objectives (SOO) to describe the government's need for contractors to propose against. An immense amount of time and energy goes into the development of those documents in order to ensure the Government acquires what it needs at a fair and reasonable price, all while ensuring competition requirements are met. The problem arises when there are unknowns in the requirements, which poses a risk to the contractor. The more risk to the contractor, the higher the cost to the government even when using a competitive acquisition strategy. A contract is a binding agreement, and a contractor can face serious consequences when it can't meet the contract requirements. Therefore, no experienced contractor will risk its reputation on a project that has too many unknown variables. This is the crux of the problem. What if the government doesn't have the answers, especially when it requires new technology? An incomplete SOW/PWS/SOO can spell trouble in this process.

The creation of OTAs was a way to explore emerging technology. OTAs were first designed to assist NASA with acquiring space age technology prototypes, and have been in use since 1958. Prototype projects must be directly relevant to enhancing the mission effectiveness of military personnel and the supporting platforms, systems, components, or materials proposed to be acquired or developed by DoD; or to improve platforms, systems, components, or materials in use by the armed forces. Prototype projects may include systems, subsystems, components, materials, methodologies, technologies, or processes. In DSS's case, this relates to enhancing the background investigation process to ensure only properly cleared personnel have access to sensitive government information and data.

The OTA process differs slightly from traditional DoD contracting methodology. The traditional approach moves slowly thorough strict procedures relating to timing and communications between the government and companies, whereas the OTA process presents potential contractors with a problem statement and allows them to present a solution brief that can be expanded upon, parsed, and refined as the technical process owners review it to ensure it meets the needs. One advantage of parsing is that it allows the government's technical experts to pick all, some, or just one piece of the solution brief meeting the needs of the government, then work with the company to expand only that part of the solution and discard the balance. It can also work in a way where two, or more, solution briefs have complementary parts that can be extracted and expanded upon to build a master solution from part of the solution briefs received. The best part is that government technical and acquisition personnel can freely exchange information with the companies throughout the process and make changes and refinements as needed.

However, DSS' initial OTA is not a blank slate, which can be used for any non-contract agreement, as it must meet at least one of the following criteria:

- All significant participants in the transaction other than the Federal Government are small businesses or nontraditional defense contractors.
- At least one third of the total cost of the prototype project is to be paid out of funds provided by parties to the transaction other than the Federal Government.
- The senior procurement executive for the agency determines in writing that exceptional circumstances justify the use of a transaction that provides for innovative business arrangements or structures that would not be feasible or appropriate under a contract, or would provide an opportunity to expand the defense supply base in a manner that would not be practical or feasible under a contract.

The prototyping process at DSS uses a three phase methodology.

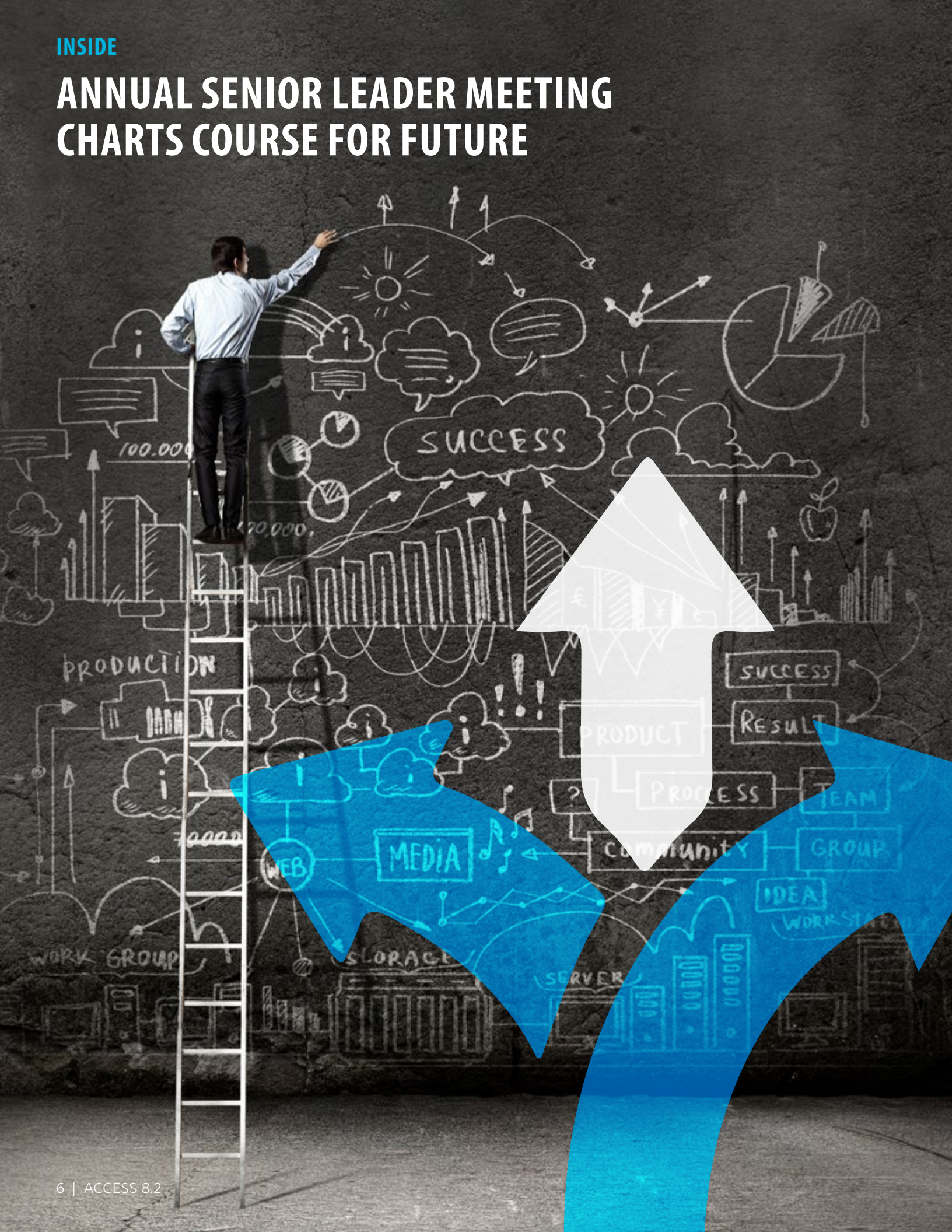
PHASE 1:	Companies solution briefs are evaluated for technical merit of the proposed concept (i.e. feasibility).
PHASE 2:	Companies whose solution briefs are favorably evaluated in Phase 1 are invited to Phase 2 where they pitch and/or demonstrate their technology in person or through submittal of additional information. In this phase, the cost is estimated, the defense utility will be detailed, how the effort fits within the definition of a prototype will be assessed, and data rights assertions are made.
PHASE 3 (PROPOSAL):	When invited to do so by the government, a company may develop and submit a full proposal. This includes a technical proposal and a price proposal.

Here is an example of how an OTA differs from a FAR/DFARS based acquisition: The agreements officer will negotiate directly with the company on the terms and conditions of the OTA, including payments, data rights, and other details that shape the agreement that will guide the company and the government through execution of the prototype. This is the opposite of a FAR/DFARS acquisition because there are strict requirements relating to communicating with offerors, data rights, payment terms and clauses.

The fascinating part of this acquisition approach is watching the innovation develop the system's features at any time throughout the acquisition cycle. The OTA process allows DSS to develop and refine business rules and processes, as the interactions with the company and the government occurs during the multiple phase OTA process. This flexibility allows the government to develop state of the art systems and processes.

INSIDE

ANNUAL SENIOR LEADER MEETING CHARTS COURSE FOR FUTURE



In keeping with recent tradition, the DSS senior leadership team took a break from day-to-day activities in mid-March and spent three days at a Senior Leader Annual Meeting (SLAM) to discuss priorities and the Director's Annual Guidance. But in a stark departure from previous such events, this year's SLAM included senior leaders from the National Background Investigations Bureau (NBIB), the DoD Consolidated Adjudications Facility, the National Center for Credibility Assessment, and the National Background Investigation Services (NBIS); all key missions and functions that will transition to DSS over the next two years.

The theme of the meeting was "Charting our Course," and the individual sessions reflected the responsibility the leadership team has to transition the new missions, but at the same time, not allow current missions to lag or fail.

In his opening remarks, Dan Payne, DSS director, said, "This is not DSS and it's not NBIB. We are taking the skill sets of both organizations and bringing them together. At the end of the day, this organization, some 13,000 strong, will be the largest and most significant security organization in the federal government."

Payne also laid out the core missions of the transformed agency:

1. **Trusted workforce**; vetting those individuals with access to national security information or access to critical technology.
2. **Protecting critical technology**; ensuring the information and technology in the hands of industry is protected.
3. **Counterintelligence**; ensuring counterintelligence runs through all major mission sets.

Payne also added that additional new missions may also move to DSS, but emphasized that DSS must first execute the current missions and do them well. "There may be future opportunities for growth, but right now we have a no-fail mission to transfer the background investigation mission," he said.

Charlie Phalen, director of NBIB, echoed many of Payne's themes in his opening remarks. "This is the largest change in the security business that I've seen in my career," he said. "I see the new mission sets by asking three questions. Do we have trusted people in our environment? Are we safe and secure in our physical environment? And, are we safe and secure in our virtual environment?"

Phalen added that the new national security environment is all about risk and how much risk leaders are willing to accept. "I think if we can explain the risk that people are taking; we can help inform the discussions," he said.

Before diving into the agenda, Payne introduced the recently approved organization chart for the Defense Counterintelligence and Security Agency (DCSA). "This is designed to force integration," he said. "We have to get away from stovepipes and develop synergies at all levels of the agency, but especially in the field."

"Transition is hard, but this is a no-fail mission and we have to get it right."

Honorable Joseph Kernan
Under Secretary of Defense for Intelligence

Payne noted that DSS currently has four regions and NBIB, three. The new organization will have five regions and each will include all mission sets. The role of the regional director will change, said Payne. "These are leadership positions," he said. "I don't expect a regional director to be an expert in all the security disciplines, I expect them to be leaders. They will have a staff of experts in each discipline."

Payne also announced that he had received approval to elevate the regional directors to Defense Intelligence Senior Level which will require the current regional directors to apply for the new positions. "My goal is to have these key leaders in place by Oct. 1, 2019."

The second day's agenda started with remarks by the Honorable Joseph Kernan, Under Secretary of Defense for Intelligence and the Honorable Kari Bingen, Principal Deputy Under Secretary of Defense for Intelligence. "There are few other enterprises more important to national security than this one," said Kernan. "Transition is hard, but this is a no-fail mission and we have to get it right."

Kernan also encouraged the leadership team to focus on what we have to do during the transfer of function while ensuring employees' needs and concerns are addressed. "As leaders, you have to remember to take care of your people."

He also discussed the current threat environment and how that is driving the need for change. "This isn't just national security," Kernan said, "it's also economic security. Our adversaries understand our vulnerabilities and we have to be out in front ahead of them, and be willing to learn and change especially in the cyber domain."

Kernan added that he wanted to elevate security within the USD(I) portfolio as security, "is just as important as anything else we do." He concluded his remarks by saying, "If we invest in security upfront, we may never have to fight."

The remainder of the SLAM was devoted to individual organizational briefs from each area, and served as an introduction and a glimpse into the size and scope of the DCSA. The final day included a discussion of the proposed integration in the field, and how the regional directors and their staffs could start preparing now and develop courses of action and options.

In closing, Payne tasked the group with looking at actions that we are taking on and ensure they will be beneficial. "Look at how we can integrate now," he said. "We want to sprint across the finish line."

Phalen noted this was the first real leadership meeting between the organizations and the first time the teams have met to discuss the future. "It's clear from this meeting that there are interdependencies at all levels. Look for synergies and how we can move forward together."

DSS BIDS FAREWELL TO DEPUTY DIRECTOR, WELCOMES NEW DEPUTY DIRECTOR

JAMES KREN

DSS Director Dan Payne (left) presents James Kren, former deputy director, with the DSS Distinguished Service Award at a farewell ceremony.

Jim Kren, DSS deputy director, was hailed at a farewell ceremony in mid-February. Kren leaves DSS after over seven years for a position with the Air Force. During the ceremony, Kren was recognized for his sage advice, calming presence and ability to balance competing missions and senior leader priorities.

DSS Director Dan Payne thanked Kren for his service and his efforts to move the agency forward. "Jim was often my sanity check," said Payne. "He helped me learn to navigate the DoD bureaucracy, which often frustrates me to no end."

Kren was also acknowledged for his concern for the workforce and how new missions or new methods would affect them. "He always put people first," said Payne.

Payne presented the DSS Distinguished Service Award to Kren for "exceptional performance and results within a complex mission space and resource-constrained environment, spearheading numerous enterprise-wide initiatives impacting the department, government stakeholders, and industry partners."

The citation also stated, "There is no DoD agency that can match the accomplishments of DSS with as few resources, and this is directly attributable to Mr. Kren's extraordinary example of leadership."

In his final remarks, Kren thanked the DSS workforce for the opportunity to lead, as well as their talent and patience. "This was a great learning environment, and I appreciate your belief and trust in me.

"I encourage all employees to trust their leadership at all levels, they care about you. I also encourage each of you to develop peer-to-peer networks to lean on and learn from each other."

CARRIE WIBBEN

Carrie L. Wibben
DSS Deputy Director

Carrie L. Wibben was appointed the deputy director in mid-February, having served as the director, Counterintelligence and Security (CI&S) Directorate, Office of the Director for Defense Intelligence (Intelligence & Security), Office of the Under Secretary of Defense for Intelligence (OUSD(I)). In that capacity, she was responsible for advising on all matters pertaining to the oversight, policy, guidance, strategic direction and advocacy for counterintelligence, law enforcement, security, and insider threat programs and resources within the Department of Defense (DoD).

She also served as the DoD lead for the Presidential post-Office of Personnel Management (OPM) breach review and implementation efforts. She had previously served as the director of Security within OUSD(I).

From 2013-2015, she was detailed from Office of the Director of National Intelligence (ODNI) to the Office of Management and Budget (OMB) where she served as the OPM Program Examiner and Senior Advisor to OMB's Deputy Director for Management/ Performance Accountability Council (PAC) chair. In this role, Wibben led the Presidential Government-wide Review following the Washington Navy Yard shooting and in March 2014, she was selected as the senior advisor for Security and Suitability Programs, a SES-equivalent position. In this role, she served as the first director of the Suitability and Security Clearance PAC Program Management Office.

Prior to her OMB detail, she was chief of the Personnel Security Group in the ODNI National Counterintelligence Executive, and she served as the senior advisor to the DNI on all security executive agent and security clearance reform initiatives. From 2011-2013, she served as the Business Unit Manager of the Interagency Joint Security and Suitability Reform Team, responsible for leading numerous clearance reform activities.

HUMAN CAPITAL MANAGEMENT OFFICE

LEADERSHIP CHANGES HANDS

LA SHAWN KELLEY

La Shawn Kelley
former chief, Human Capital Management Office

DSS bid farewell to La Shawn Kelley, chief of the Human Capital Management Office, who departed DSS after 10 years for a detail to NATO. In a ceremony in mid-February, Kelley was recognized for her contributions to DSS to include establishment of the Director Award Program, relocations under Base Realignment and Closure legislation, a move to the Defense Civilian Intelligence Personnel System, as well as serving as a coach and mentor.

DSS Executive Director Troy Littles presented Kelley with the DSS Distinguished Service Award. The citation noted that, "throughout her tenure as chief, Human Capital Management Office, Kelley demonstrated exceptional leadership and a record of achievements that have had a tremendous impact on the agency and its geographically dispersed workforce."

Kelley was also recognized as "a forward-thinking and engaging leader. Kelley built partnerships and common understanding to achieve strategic goals and positively influence enterprise-wide human capital decision-making."

In a farewell letter, Dan Payne, Director, said "since joining the Defense Security Service nearly ten years ago, you have made important and lasting contributions and have been a tremendous asset to this agency … you can take great satisfaction in knowing that your efforts have put DSS on a solid path for the future. Congratulations on your detail!"

ELIZABETH C. HOAG

Elizabeth C. Hoag, chief,
Human Capital Management Office

Joining DSS as the new chief of HCMO is Elizabeth C. Hoag, who is on detail from the Office of the Under Secretary of Defense for Intelligence. She joined DSS from an assignment as the senior policy advisor, Human Development Directorate, National Geospatial-Intelligence Agency (NGA), where she was responsible for human capital policy solutions and designed, developed and managed the eNGAge program, NGA's innovative geospatial exchange program with industry.

She was promoted to Defense Intelligence Senior Level in July 2006, upon selection as the deputy director for Human Resources/ Defense Civilian Intelligence Personnel System (DCIPS) program manager. In this role she was responsible for the design, development, evolution and sustainment of this unique personnel management system serving approximately 60,000 Defense Intelligence employees. She led the DCIPS Working Group members from across the enterprise, and supervised the personnel team in HCMO, overseeing executive resources, policy, DCIPS implementation and training staff and contractors. Hoag served as the Department's implementation lead for Presidential Policy Directive 19 – "Protecting Whistleblowers with Access to Classified Data."

Hoag began her government career with the Department of the Navy, Naval Criminal Investigative Service, where she supervised the personnel team in the Career Services Department, responsible for supporting approximately 1,400 civilians. She then joined NGA where she served in Human Resources as a policy lead and as the Executive Resources program manager, and in the Office of the General Counsel as an executive officer, law clerk and attorney.

A Q&A WITH PATRICIA STOKES

Patricia Stokes, a member of the Defense Intelligence Senior Executive Service, is the Director of the Defense Vetting Directorate (DVD). In this capacity, Stokes is responsible for the implementation of the transfer of the background investigation mission from the National Background Investigations Bureau (NBIB) to DSS and operationalizing and deploying the National Background Investigation Services (NBIS). Prior to this assignment, she held federal positions in the three military departments, two defense agencies, and a combatant command, culminating in her position as Director of Security for the Department of the Army as the Senior Security Advisor in the Office of the Deputy Chief of Staff for Intelligence. In that position, she was instrumental in leading several personnel security reform initiatives for the DoD.

Q What led you to this position?

A I consider myself a change agent and advocate for continuous improvement. Before coming back to DSS, I spent the last 10 years of my career as the Director of Security on the Army Staff. In this position, I led significant change in several personnel security reform efforts. The Army was a driving force in the piloting of Continuous Evaluation (CE) that was foundational in major policy reform initiatives and Trusted Workforce 2.0. As the largest military department, the Army led the CE effort. Additionally under my tenure, the Army centralized its background investigation submissions which reduced errors by 28 percent, streamlined the process, established consistently repeatable processes and metrics for measuring progress and pain points. This model and many lessons learned are being used in establishing the next generation system. We also learned that transparency and communication with the stakeholder base is absolutely critical. So when the opportunity at DVD presented itself, it seemed like a natural next step.

Q What should we know about the Defense Vetting Directorate?

A The Directorate was stood up in April 2018, just over a year ago. The original mission was to prepare DSS and the Department to take back the DoD portion of the background investigative mission in accordance with the FY18 National Defense Authorization Act. Since then, the focus has shifted to a 100 percent transfer in accordance with Executive Order 13869. My direction is now to move into transition on the way to transformation of the personnel vetting enterprise. We are focused on personnel vetting transformation and reform. To that end, we are hiring personnel with unique skill sets; change agents, data scientists, forward-thinking subject matter experts and the like. We are very focused on collaboration with our stakeholders and our system developer. We are the single NBIS functional requirements owner and our job is to gather and vet stakeholder requirements from across the federal government and manage the governance of the Information Technology capability and federal-wide personnel vetting operations.

Q What have you and the DVD accomplished in the past year?

A My first priority was, and still is, to hire the right people. I have also been very focused on establishing close relationships with the NBIB team and the NBIS Program Executive Office (NBIS PEO). NBIS is the personnel vetting system of the future. We have established a very close partnership with them with the goal of maximizing state of the art technology, such as, artificial intelligence and machine learning. We have really focused on creating what we call our Enterprise Business Support Office which is critical to all activities associated with deployment of our new information technology capabilities — our bread and butter. We are engaging with the military and non-DoD stakeholders to ensure we are capturing their requirements, mapping new business processes, initiating pilots to test new investigation methodologies, etc. We are also implementing executive correspondence and authorities provided by the Executive Agents. The team is implementing Continuous Evaluation, building the construct for Continuous Vetting in concert with Trusted Workforce 2.0 policy issuance, integrating the DoD Consolidated Adjudications Facility into the DVD, and established and implementing a capability for the new Expedited Screening Protocol to address foreign associations and influence in the investigation process. So, in short, we've been busy.

Q What are the most significant challenges you are facing?

A Resources, both people and money are always a concern and you never seem to have enough. But a larger, less tangible challenge, is managing change. We are dealing with a cultural shift in the transition and transformation of our business processes. It is change management 101 and requires stakeholder buy in. All stakeholders, internal and external. Discomfort is where change happens and forces us to adjust. With our system developer, we must get it right rather than getting things done fast. This requires patience in an arena that expects and is demanding change yesterday. It requires resilience on our part and excessive communications with our stakeholders. It's really about managing expectations but also delivering.

Q How are you integrating the disparate organizations and workforces within DVD into a cohesive whole?

A First, we strive to ensure everyone on the team has the same fundamental understanding of what we are doing. I also don't think you can ever over communicate. I have to ensure everyone in the enterprise has a foundational understanding of where we are going, why, and what we want to achieve. I want to ensure every member of the team understands the value they bring and their contribution and importance to the enterprise.

Q Not only is the organization (DSS) set to change, but many of the existing procedures and processes are set to change as well. Can you elaborate on some of those as they relate to personnel vetting.

A As I said, we want to leverage technology and automation to streamline the end-to-end vetting process from submission through continuous vetting. Much of the new process will be defined by the Trusted Workforce 2.0 initiative which is looking at different vetting scenarios based on mission needs and risk in person and position. It is really a move away from a one size fits all mentality to one based on risk and mission requirements.

Q What is the difference between continuous evaluation and continuous vetting?

A Continuous evaluation uses a set of automated record checks and business rules to focus on the background of someone with clearance eligibility. Continuous vetting will include continuous evaluation, agency and local information (insider threat, human resource, inspector general), plus time and event driven checks based on risk level. It is a real-time review of someone's background at any given time to determine their continued eligibility and suitability. Continuous vetting will eventually satisfy the requirements for periodic reinvestigations and, as I mentioned, will also apply to the suitability community.

Q What is the biggest change you've seen in the personnel vetting mission?

A I believe this is it. Right now we are poised to fundamentally redesign the personnel vetting mission. It's exciting and we will deliver!

Q What are the biggest lessons you learned during the transformation of the personnel security investigation submission process for the Army that can be applied to DSS?

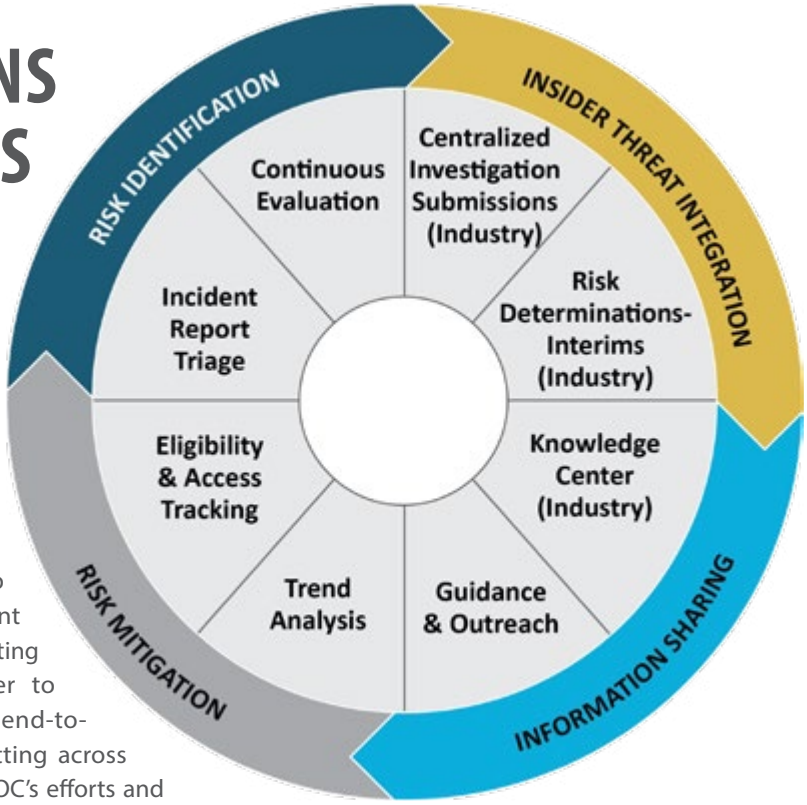
A You have to start by co-opting the naysayers and turning them into your advocates. Communicate, communicate, communicate and most of all, deliver results.

Q Any other thoughts?

A I am excited and honored to be part of this once in a lifetime reform. I think I have been afforded this opportunity because I had leaders who believed in me and gave me the chance to take calculated risks. I've had exceptional leaders whose behavior I believe I've tried to emulate. I want to bottle that up and model it for my team and create the next generation of innovative thought leaders who are never satisfied with the status quo and always push for better government.

VETTING RISK OPERATIONS CENTER MISSION EVOLVES

by Lynette Akers
Defense Vetting Directorate



Over the past few years, the Vetting Risk Operations Center (VROC), formerly known as Personnel Security Management Office for Industry (PSMO-I), mission set has evolved significantly.

The VROC is a consolidation of PSMO-I, the DoD's Continuous Evaluation Program Management Office, and the Industry Insider Threat Office. Through this consolidation, VROC is directly contributing to efforts underway within the Department to align processes across the enterprise and ultimately implement a continuous vetting program to manage the DoD trusted workforce for the duration of the time an individual has access to mission, people, information, and property.

VROC is playing a critical role in personnel security reform by leading the Continuous Evaluation (CE) Program for the DoD

VROC also provides analytic and adjudicative support for the DoD Consolidated Adjudications Facility to streamline adjudicative functions, and consolidate analytical and administrative activities. Additionally, the VROC has direct linkage to the Defense Insider Threat Management and Analysis Center for expeditious information sharing to the Department's Insider Threat programs.

The VROC is part of the newly established Defense Vetting Directorate (DVD), whose portfolio will align all current and future DSS vetting functions in order to provide holistic end-to-end personnel vetting across the enterprise. VROC's efforts and partnerships enhance timely information sharing, achieve efficiencies, and strengthen overall readiness for the Department.

VROC is playing a critical role in personnel security reform by leading the Continuous Evaluation (CE) Program for the DoD. Efforts are underway to transform the historical background investigations process to be an event and data driven model, thereby enhancing the standard periodic reinvestigation (PR) process by detecting adjudicative-relevant information prior to using automated record checks, tiered-query capability and integrated reporting in near real time.

In FY18, with the current CE population of 1.2 million enrollees, VROC received over 47,000 alerts from automated records checks. Of those alerts, 30 percent contained derogatory information not previously known. CE is detecting issues for the enrolled Secret population 6 years and 7 months before the next scheduled traditional PR. On average for the enrolled Top Secret population, CE detects issues 1 year and 5 months before the next scheduled traditional PR. Early detection often creates opportunities for positive intervention – helping personnel resolve their issues before it is necessary to remove them from access or revoke their clearance.

Additionally, the VROC workforce has contributed to the deferment of over 11,000 industry cases into the CE risk mitigation program following the Director of National Intelligence Trusted Workforce Vetting Executive Correspondence guidance. VROC is projected to defer another 37,000 cases in FY19, further balancing risk identification/mitigation with cost savings. The deferments also play a key role in reducing the DoD vetting stakeholders' pending inventory.

With the goal of increasing the CE population further beyond the 1 million goal and ongoing efforts to enhance the vetting information sources, it was critical to increase staffing to support mission requirements. Last year, VROC held a hiring event to bring on new personnel, doubling the size of the VROC office, and will hold another hiring event this summer to accommodate the future mission expansion to align resources with the CE population growth.

THREE CORE CERTIFICATIONS APPROVED FOR RE-ACCREDITATION

by Jason Taylor
Center for Development of Security Excellence

The Security Professional Education Development (SPēD) Certification Program's three core certifications (Security Fundamentals Professional Certification (SFPC), Security Asset Protection Professional Certification (SAPPC), and Security Program Integration Professional Certification (SPIPC)) were successfully approved for re-accreditation by the National Commission for Certifying Agencies (NCCA) in November 2018.

The SPēD certification program, which is run by the Center for Development of Security Excellence, ensures there exists a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals.

This effort marks the first time any federal government entity has accomplished the stringent and rigorous NCCA re-accreditation application process, not for just one re-accreditation, but for three SPēD core certifications. Initially, NCCA accredited SFPC in December 2012, SAPPC in January 2014 and SPIPC in February 2015.

With the re-accreditation, all three certifications have been extended an additional five years.

With the re-accreditation, all three certifications have been extended an additional five years. "This results in a strategic position that supports the security workforce," said Kevin Jones, CDSE director, "and ensures we provide a competitive advantage to the security workforce and profession, and continue to increase security enterprise integration across the federal government."

Additionally, this accomplishment was recognized by the Honorable Joseph Kernan, Under Secretary of Defense for Intelligence, through an official memo, who commended "CDSE on its lessons-learned which will be invaluable for all other DoD certification programs in the future."

CREATION OF NATIONAL ACCESS-ELSEWHERE SECURITY OVERSIGHT CENTER UNDERWAY

The National Access-Elsewhere Security Oversight Center (NAESOC) is on its way to becoming a reality in late 2019. The goal of this initiative, developed by the Industrial Security Field Operations Directorate, is to transfer oversight of select non-critical technology facilities away from the field and into the NAESOC, which will result in balancing the workload across field operations. This process will enable the field to focus more effectively on Critical Technology Protection, conducting Comprehensive Security Reviews and actively monitoring Tailored Security Plans, in addition to building stronger partnerships with industry and government customers.

Another benefit to Access-Elsewhere facilities is that the NAESOC will provide continuous outreach and consistent direction.

The NAESOC initiative is the direct result of senior leaders seeking solutions for the field to focus on higher-risk technology protection and to brainstorm ideas for oversight of Access-Elsewhere facilities of lower-risk programs; those not identified as working on critical assets, and where access is often at the prime contractor or government customer location. This resulted in the creation of two different working groups -- the Access-Elsewhere Strategy Working Group and the Non-Professional Services Working Group, who developed the Access-Elsewhere oversight center concept.

Currently, the NAESOC initiative is jointly led by Field Office Chiefs Julia Ruffini and Kathy Kolwicz in the Capital Region, along with representatives across multiple directorates grouped into one large encompassing working group led by Industrial Security Specialist Sarah Beauregard. The Project Champion is Justin Walsh, Regional Director, Capital Region. The working groups are currently working on several large tasks centered around the NAESOC structural design, and identifying criteria that would determine the facilities that should be transferred to the NAESOC, the facilities that should remain in the field, and the determination point on when an in-process facility should enter the NAESOC. The working groups are also developing a concept of operations and standard operating procedures (SOPs) for the NAESOC. The NAESOC team anticipates conducting a pilot program which will include execution and testing of the SOP, and a subset amount of facilities in the July 2019 timeframe.

INAUGURAL INTERNATIONAL FOCI CONFERENCE HIGHLIGHTS SHARED FOCI EXPERIENCES, BEST PRACTICES

by Syeda Borchmeyer and Marguerita Ramirez
Industrial Security Integration and Application

In November 2018, DSS held its inaugural International Foreign Ownership, Control, or Influence (FOCI) Conference for European and Middle Eastern companies operating under FOCI mitigation agreements, at the National Museum of the Marine Corps in Quantico, Va. DSS organized this conference in response to feedback from FOCI partners requesting a forum for foreign shareholder engagement. Attendees included senior executives of foreign parent companies, Government Security Committee chairpersons, representatives from law and consulting firms, and stakeholders from across the U.S. government.

In his opening remarks, Garry P. Reid, Director for Defense Intelligence (Intelligence & Security), Office of the Under Secretary of Defense for Intelligence, described the current global security landscape on an international level, while highlighting the threat certain adversaries pose to the United States and its industrial base. He explained how adversaries are open in their desire to engage in power competitions, and are actively investing in such objectives. The United States is then faced with national security concerns when countries steal U.S. technology secrets, and while the nation might not be able to stop all threats from our adversaries, we must always attempt to mitigate risks.

A panel on Foreign Direct Investment: Trends and Analysis covered the landscape for international investment and the future of foreign direct investment in the context of the Foreign Investment Risk Review Modernization Act. Enacted in 2018, this law introduced significant reforms to the processes and authorities of the Committee on Foreign Investment in the United States (CFIUS). Participants were assured that despite policy reforms and increased attention to national security concerns, the Defense Industrial Base (DIB) is still amenable to business interests, ripe with opportunities for investment, and welcoming of multinational corporations. David Fagan, Covington and Burling LLP, explained that he continues to advise his clients that the United States is still open for business, even as CFIUS evolves in its approach evaluating the impact foreign investments have on the DIB.

Dario Deste, chief executive officer, Fincantieri Marine Group, gave a presentation on how investing in security can lead to financial growth for FOCI-mitigated companies. Deste offered two key takeaways on making security

Dustin Dwyer (center), Industrial Security Integration and Application (ISIA), participates in a panel discussion on FOCI theory and application, along with Ben Richardson (left), Office of the Under Secretary of Defense for Intelligence, and Stefanie McCabe, ISIA. (Photo by Marc Pulliam, CDSE)

Chris Nissen, The MITRE Corporation, explains the goal of Deliver Uncompromised - to provide warfighting capabilities to operating forces without compromising critical information. (Photo by Marc Pulliam, CDSE)

profitable: invest in security, as it can be a business enabler rather than a cost center; and invest in the FOCI company's operations. Deste stressed that shareholders' investment in security and FOCI companies leads to a better security program, and is better for the company and shareholder's business. As he stated, "No business can succeed without understanding what a customer needs. When we fail to be security cognizant, we'll be out of business. The objective is to make America stronger."

A panel on FOCI mitigation topics urged participants to understand that, while FOCI mitigation can be a frustrating process, it rests on a sound policy foundation and strives to strike a balance between national security interests and a company's business requirements. FOCI mitigation is increasingly dynamic and focused less on bright-line rules, and more on effectively mitigating and reducing the overall risks arising from foreign control or influence. As a result companies now have greater flexibility when they demonstrate risks have been sufficiently mitigated.

During his keynote address, DSS Director Dan Payne noted that, since World War II, every advantage the United States has maintained on the battlefield has been as a result of technological advancements. He reiterated that adversaries continue to target the DIB because that is where technological innovations emerge. As he further noted, in order to be successful, industry must at times do business with U.S. adversaries. Therefore, "cookie cutter" security programs are no longer effective and must evolve to face the current threat environment.

Initiatives for security programs, such as Deliver Uncompromised, were extensively discussed during the conference. Chris Nissen, director, Asymmetric Threat Response, The MITRE Corporation, informed the audience that the enterprise goal of Deliver Uncompromised is to provide warfighting capabilities to operating forces without compromising critical information. He noted that the U.S. government spends a significant amount of funds on acquisitions, but it is rarely recognized that the resulting products need to be delivered in a pristine state. Cost, schedule, and performance are the typical guiding factors in the acquisition process, but Deliver Uncompromised seeks to add security to the key variables in that equation, thereby incentivizing industry to implement robust security program so that their bids will be more competitive, he concluded.

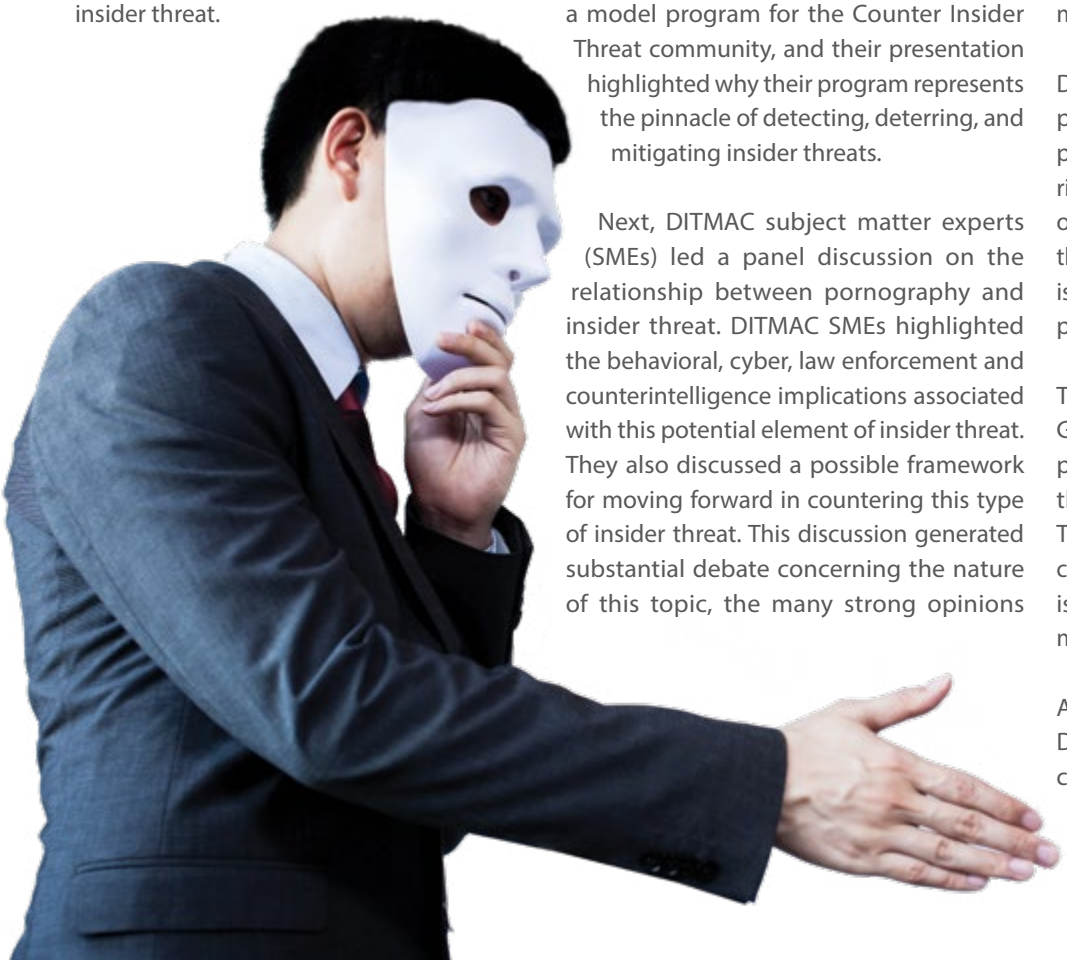
The final panel discussed the relationship between Government Security Committees and corporate C-suites. Panelists offered perspectives, best practices, and experiences of both outside directors and proxy holders, as well as foreign shareholder representatives, on the dynamics affecting FOCI Boards. In one exchange, Daniel T. London, group chief executive, Health and Public Services, Accenture plc, explained to foreign shareholders that positioning a FOCI company to be successful should be the top priority of a parent company. Gerald Amann, general counsel, Accenture Federal Services (AFS), commented on the support, understanding, and engagement of the foreign shareholder in AFS's efforts to maintain an outstanding security program and transition to a different FOCI mitigation agreement.

Participants judged the conference a success. DSS looks forward to further dialogue with industry at the next IFC in summer 2019.

FORUM EXPLORES HUMAN SIDE OF INSIDER THREATS; DISTINGUISHING BETWEEN DIFFICULT, DANGEROUS

by Ashley Abrams
DoD Insider Threat Management and Analysis Center

In January 2019, the DoD Insider Threat Management and Analysis Center (DITMAC) hosted the inaugural "Human Side of Insider Threat Forum," which was designed to focus on insider threats that are not easily detected by or mitigated with technology. Experts from across the Counter Insider Threat community presented on a variety of topics, to include workplace violence, mental illness, suicide, pornography and distinguishing between "difficult" and "dangerous" employees. Presenters and attendees collectively shared experiences, case studies, and discussed the importance of sharing information and best practices to advance the insider threat mission. In addition, the attendees provided recommendations to consider for the way forward in countering the human side of insider threat.



The forum, although occurring in the midst of the partial government shutdown, was attended by over 230 insider threat professionals from 60 different government agencies who actively engaged in discussions, questions and answers throughout the day's presentations.

The Naval Criminal Investigative Service (NCIS) Insider Threat Division kicked off the program with an overview of the methodology they employ to differentiate between "difficult" and "dangerous" employees. Their presentation and case studies discussed various approaches for insider threat programs to consider when advising leaders on options available to mitigate concerning behavior. The NCIS Insider Threat approach has been a model program for the Counter Insider Threat community, and their presentation highlighted why their program represents the pinnacle of detecting, deterring, and mitigating insider threats.

Next, DITMAC subject matter experts (SMEs) led a panel discussion on the relationship between pornography and insider threat. DITMAC SMEs highlighted the behavioral, cyber, law enforcement and counterintelligence implications associated with this potential element of insider threat. They also discussed a possible framework for moving forward in countering this type of insider threat. This discussion generated substantial debate concerning the nature of this topic, the many strong opinions surrounding it, and the unchartered territory of discussing pornography as a potential insider threat concern.

Speakers from the DoD Consolidated Adjudications Facility (CAF) and Defense Suicide Prevention Office (DSPO) tackled mental illness and insider threat from two different viewpoints. The CAF presentation focused on mental health from a security clearance perspective and reiterated that mental illness falls under the current adjudicative model that concentrates on the whole-person concept. DSPO provided insight on how to understand the threat to one's self, how it fits into the scope of an insider threat, and how to incorporate the information into an insider threat hub mitigation strategy.

Dr. Russell Palarea, consulting operational psychologist, Diplomatic Security Service, presented on managing workplace violence risk. Dr. Palarea discussed key building blocks of threat management, which emphasized that information-sharing between disciplines is critical to a successful threat management/prevention program.

To close out the forum, the U.S. Coast Guard's Threat Management Unit (TMU) presented a case study that incorporated the topics discussed throughout the day. The TMU reiterated a prominent theme - a coordinated response from every department is paramount to a successful insider threat mitigation strategy.

At the request of the collective attendees, DITMAC plans to host additional forums covering emerging insider threat topics.

USE OF SECURE VTCS EXPANDS OUTREACH TO CLEARED INDUSTRY

by Sarah Alcantar and Andrew Woods
Counterintelligence Directorate

Partnership with Industry to Protect National Security is not just a fancy tagline, it's the mission of the Counterintelligence Directorate Strategic Engagement (SE) Division. Through the CI Partnership with Cleared Industry program and monthly Secure Video Teleconference (SVTC) initiative, the division works on increasing DSS efforts to foster CI engagement and classified information sharing with cleared industry, setting the conditions for uncompromised delivery of classified technologies and services for the warfighter.

A critical element to achieve this goal is the expansion of secure communication capabilities between industry-government and DSS-government. The agency's initiative of embedded secure video terminals within DSS field offices was a significant step towards the SVTC initiative.

THE BEGINNING

In fiscal year 2015, Strategic Engagement successfully conducted two SVTCs with cleared industry with support from the Office of the Chief Information Officer (OCIO) and Office of Security. At the time, DSS connected to 24 SVTC terminals at 21 field offices and one external government partner location. Given the initial success, SE was instructed to develop a plan to engage with industry, academia, law enforcement, the Intelligence Community and other federal and non-federal partners on a quarterly basis. The initial SVTC attendance averaged 200 participants. In each of the first three quarters of fiscal year 2016, industry's participation doubled to approximately 400, and the upward trend continues.

It was difficult in the beginning, as SE tried to minimize the impact on the DSS support offices, while simultaneously trying to identify topics, guest briefers, establish a reoccurring schedule and feedback forms, and identify an invitation tracking system. CI validates topics of discussion, and established a schedule where the third Thursday of every month, is the SVTC day. In fiscal year 2017, the SVTC with cleared industry transitioned from a quarterly event to a monthly occurrence.

INITIAL OPERATING TO FULL OPERATIONAL

In the introduction of the 2017 "Targeting U.S. Technologies" report, DSS Director Dan Payne wrote, "DSS' application of the threat knowledge in the Trends publication and other DSS products is vital as we transition from a process focused on policy compliance to an intelligence-led, asset-focused and threat-driven approach to protecting national security information and technology."

As the agency moved forward with the initiative, the intent was to leverage SVTC nodes within cleared industry and the federal government to accommodate larger audiences. In fiscal year 2017, the SVTC with cleared industry reached a milestone with an average of 400 attendees per month across 55 DSS field offices, six interagency sites, three University Affiliated Research Centers and five cleared industry sites.

In addition, the SVTC hosted briefers and subject matter experts in fiscal year 2017 from the CIA, National Security Agency, FBI, Department of Homeland Security Homeland Security Investigations, Air Force Office of Special Investigations, National Counterterrorism Center, the National Counterintelligence and Security Center, Naval Criminal Investigative Service, and Marine Corps Intelligence Activity.

For fiscal year 2018, the SVTC continued its success and reached over 4,430 registered participants with an average of 403 attendees each month. Briefing topics were provided by CI, the Center for Development of Security Excellence, Operations Analysis Group, Industrial Security Field Operations, and 12 interagency partners, to include the Department of Energy and the Department of State.

THE WAY AHEAD

To date, almost all DSS facilities with SVTC capability have participated, as have an increasing number of industry partner facilities. The feedback from industry and government leaders has been largely positive. Based on recent SVTC feedback, CI has received reporting from cleared industry that security/force protection postures are in process for revision based on a recent Defense Intelligence Agency briefing. In another instance, a cleared facility reported they now have access to technical points of contact they never knew existed based on a guest briefing from the Department of State. Bottom-line, the information presented at the SVTC has proven valuable to cleared industry and other attendees. The SE Division will continue to strive to provide relevant and timely briefing topics in fiscal year 2019 and increase attendees each month.

DSS, E2C2 PARTNERSHIP HELPS DETECT, DETER, DISRUPT THREATS

by Mike Shydlinski
DSS Liaison to Export Enforcement Coordination Center
Counterintelligence Directorate

In May 2012, then DSS Director Stan Sims attended a ribbon cutting ceremony to mark the opening of the Export Enforcement Coordination Center (E2C2). "I am excited for DSS to be recognized as one of the key participants of this national-level operation," said Sims. "This is another example of other federal agencies beginning to recognize the value that DSS brings to the security, intelligence, counterintelligence, and law enforcement communities."

The Counterintelligence Directorate Strategic Engagement (SE) Division provides a liaison officer (LNO) to E2C2 to ensure that DSS suspicious contact reports related to violations of U.S. export control laws involving cleared industry are reviewed by participating agencies.

The LNO responds to inquiries submitted by the investigative agencies which routinely involves answering questions about facility and personnel clearances, identifying which technologies may be at risk, and coordinating communication between DSS field personnel, facility security officers, and federal law enforcement officials. The LNO also reviews all DSS SCRs for potential export enforcement information and provides referrals to other government agencies to take action on.

The E2C2 is administered by the Department of Homeland Security (DHS) with a leadership team comprised of officials from DHS, the FBI, and the Department of Commerce.

Established under Executive Order 13558 in November 2010, the E2C2 is responsible for enhanced information sharing and coordination between law enforcement and intelligence officials regarding possible violations of U.S. export controls laws. The E2C2 is the primary forum within the federal government for information and intelligence sharing related to export enforcement and proliferation matters. The E2C2 leverages partnerships from 17 agencies across the federal government such as the Office of the Director of National Intelligence, and the departments of Justice, State, Treasury, Defense and Energy. There is also representation from the Commerce Department's Bureau of Industry and Security, U.S. Customs and Border Protection, Defense Criminal Investigative Service, and the National Nuclear Security Administration. The mission of the E2C2 includes de-confliction and coordination of export control enforcement activities.

This helps partner agencies detect, prevent, disrupt, investigate and prosecute violations of U.S. export control laws.

The E2C2 serves as the primary forum within the federal government for executive departments and agencies to coordinate and enhance their export control enforcement efforts. The center maximizes information sharing, consistent with national security and applicable laws. This helps partner agencies detect, prevent, disrupt, investigate and prosecute violations of U.S. export control laws.

DSS partnership with E2C2 and U.S. Immigration and Customs Enforcement Homeland Security Investigations (HSI) Counter-Proliferation Investigative (CPI) Program supports DSS's need to continue to increase objective outreach and engagement to detect, deter and ultimately disrupt threats. HSI's CPI Program mission is to prevent illicit procurement networks, terrorist groups and hostile nations from illegally obtaining United States origin technology, materials and components that can be used in the development of conventional, non-conventional, and improvised weapons and weapons systems. These partnerships support the SE Division's effort of fostering collaboration and information sharing that enables faster, more efficient and effective protection of critical capabilities and technologies.

A recent success story from a DSS referral involves HSI. "HSI's overall counter-proliferation mission is to prevent hostile nations, foreign adversaries, terrorist networks, and transnational criminal organizations from obtaining materials that threaten the security of the United States and its allies," said HSI Special Agent Ryan Babcock. "The strategic partnership between HSI and DSS enhances our mission and has resulted in some of the most significant counter-proliferation investigations conducted by our agency. In fact, one of the most memorable investigations I participated in, which encompassed a sophisticated undercover operation targeting an individual attempting to acquire controlled communication equipment from a cleared contractor, was initiated based on information provided by DSS.

"Without question, continued collaboration between our agencies strengthens our national security efforts against those who attempt to illegally acquire our most sensitive technology and military equipment," Babcock concluded.

NO TYPICAL DAY FOR DSS LIAISON TO FBI

Editor's Note: *The following reflects the thoughts and opinions of the author on the role of the DSS liaison to the FBI.*

by Brian Medley
Counterintelligence Directorate

As the DSS liaison to the FBI headquarters, the most satisfying aspect of the job is that there is no typical day. The mission, however, is consistent: ensure the suspicious activity DSS identifies that is directed at cleared industry -- whether by foreign actors or potential insiders -- is routed to the appropriate elements within the FBI; and, support the FBI in its investigations of a whole range of potential threats to cleared industry. This support, both to DSS and the FBI, takes a variety of forms and has given me greater appreciation for the positive impact the DSS-FBI partnership has on national security.

A majority of my time is divided between two tasks. The first is reviewing DSS suspicious contact reports (SCRs). Most of the SCRs that DSS generates do not result in a case, even if they do contribute to increasing our overall knowledge of potential adversaries. A minority of those reports, however, represent viable opportunities to take action against identified threats, and sometimes these are exceptionally time sensitive. On one occasion, for example, a cleared industry employee notified a DSS counterintelligence special agent that it appeared an employee had stolen sensitive data and was attempting to leave the United States. Working with various FBI headquarters elements, we were able to notify the relevant FBI field office and the FBI was able to intercept the individual at the airport.

The second task is fielding requests for information and assistance from the FBI and DSS. This aspect of my role is interesting as it allows me to play at least a small part in cases from all over the country and sometimes the world. FBI requests typically involve helping to identify a point of contact within industry or DSS, a review of specific kinds of suspicious activity directed at specific targets, or the review of data related to subjects of investigations who have or had security clearances. Occasionally, however, it is a little outside the box. On one occasion, an FBI special agent contacted me to ask about a cleared employee's clearance. DSS personnel, in the course of normal business, had identified that a cleared employee appeared to have no reason to maintain a clearance and began the process to remedy the apparent oversight. It turned out, however, that the employee was assisting the FBI in a sensitive task for which they required access to classified information. Far from being upset about the clearance issue, the agents working on the case were appreciative that the matter had been detected. With a little work, we were able to coordinate the employee's continued access and enable him to finish the critical project.

Sometimes the satisfaction I get from the job is institutional. I have always been impressed by the professionalism of everyone at DSS, but sometimes even dedicated professionals make mistakes. On a number of occasions, DSS has forwarded proposals to suspend an employee's clearance, based on suspicious data. Every now and then, however, I find through FBI channels that the data had been reported in error or had been misinterpreted. In those cases, we are able to coordinate with the appropriate FBI headquarters elements for release of the corrected record. Getting "it" right and, in some cases, preserving someone's career from an unnecessary stain, is every bit as satisfying as participating in the opening of an investigation.

While interagency partnerships aren't always smooth, I can tell you that my experience as the DSS liaison has been uniformly positive. Just about every FBI employee I have interacted with not only appreciates DSS, but is anxious to work with us. They are equally enthusiastic about developing positive relationships with cleared industry and working collaboratively to address threats.

DSS EMPLOYEE IS THE SECOND STUDENT TO EARN ALL FIVE CDSE EDUCATION CERTIFICATES

by Julie Wehrle
Center for Development of Security Excellence

DSS Director Dan Payne (left) presents Juaquita Gray, San Francisco Field Office, with the Certificate for Systems and Operations.

Juaquita Gray, a senior industrial security representative in the San Francisco Field Office, is the second Center for Development of Security Excellence (CDSE) student and the second DSS employee to earn all five CDSE Education Certificates offered by the CDSE Education Program.

Gray earned her first two Education Certificates, the Certificate in Security Leadership and the Certificate in Risk Management, in 2015, followed by the Certificate in Security (Generalist) and the Certificate in Security Management in 2016. She earned the last one, the Certificate for Systems and Operations, in May 2018.

The CDSE Education Program offers a curriculum of advanced and graduate courses designed specifically to broaden DoD security specialists' knowledge and understanding of the security profession and prepare them for leadership positions and responsibilities. The virtual instructor-led courses are all tuition free. Students can earn Education Certificates by successfully passing four CDSE Education courses in any of five concentrations.

THE FIVE EDUCATION CERTIFICATES ARE:

Certificate in **Risk Management**

Certificate in **Security Leadership**

Certificate in **Security Management**

Certificate in **Security (Generalist)**

Certificate for **Systems and Operations**

Prior to starting her DSS career in 2012, Gray supported national security on active duty in the U.S. Air Force and positions at several cleared defense contractors. She credits fellow DSS coworker and information systems security professional Curtis Cook with introducing her to the CDSE Education program and leading by example when he became the first student to earn all five Education Certificates. Gray initially planned to take only the Effective Communication in DoD Security course and then move on to another educational program.

"After discovering the high-caliber content of the curriculum, student focused instructors, and user friendly virtual instructor-led classroom, I realized the remaining CDSE Education courses and the graduate-level certificate programs were very appealing," Gray said. "The program content was entirely conducive for self-improvement and having greater impact as a security professional."

She said that the quality and value added curricula "directly supports professional advancement as a result of the increased DoD security knowledge base and the analytical and critical thinking performance capabilities."

As a result of the CDSE Education courses, "I feel that my professional interactions with industry have definitely benefited." For instance, Gray said that the Understanding Adversaries and Threats to the United States and the DoD course is in direct alignment with DSS in Transition's (DiT) 12X13 Method of Contact Method of Operation - Threat Matrix. The curriculum examined intentions and capabilities of America's most significant adversaries and delivered insight of the multifaceted concept of threat. As a result of this course, she developed a better understanding of threat objectives and capability to more effectively relay a vivid depiction of these risks while briefing the security staff during enhanced security vulnerability assessments.

Field Office Chief Kevin Flowers, Gray's supervisor in the San Francisco Field Office, said that "critical thinking is vital to success of DiT. He said that more responsibility and operational control continues to move to the field.

"Critical thinking skills directed to problem solving is not just the responsibility of the field office chief, it is everyone's responsibility," he said. "The success of a field office and the impact it can have in the protection of critical technology will depend on critical thinking and collaboration among the team and among our industry partners."

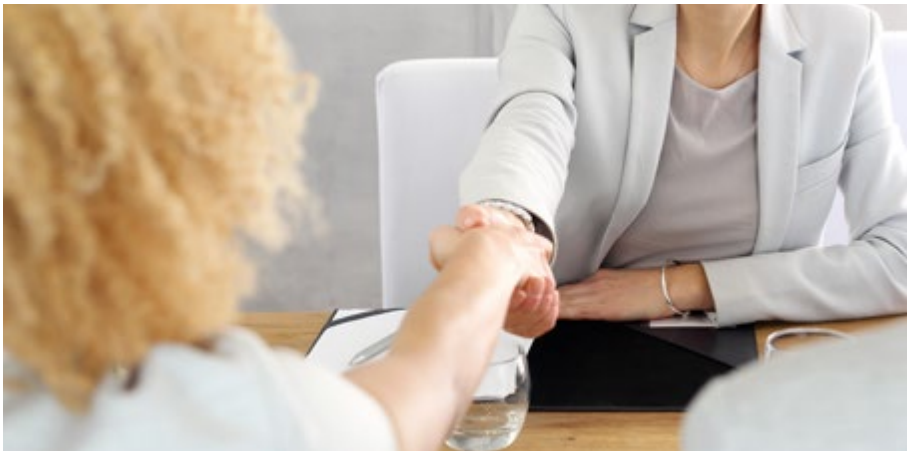
Gray said her goal is to be "ever-learning" and that she believes continuous learning should be an aim for everyone. She plans to continue encouraging her colleagues and coworkers to participate in the program.

PANEL DISCUSSION FOCUSES ON NEED FOR INCREASING INNOVATION

DSS Deputy Director Carrie Wibben served as a panel member at Georgetown University's Center for Security Studies in mid-April. The panel was entitled "Innovation in the Midst of Great Power Competition." Panelists also included (left to right): Chris Taylor, moderator, Wibben; Gen. Stephen Wilson, Vice Chief of Staff of the U.S. Air Force; Dr. Sarah Sewall, former Under Secretary of State of Civilian Security, Democracy and Human Rights; and the Honorable Robert Work, former Deputy Secretary of Defense. The Georgetown Security Studies program is congressionally funded graduate level program designed to have students address national security challenges. The audience for the panel included students enrolled in the program, other Georgetown professors and students, and was open to the media. The discussion focused on the premise that the United States is engaged in a competition with China for military and economic supremacy, and the United States is lagging behind in recognizing and addressing the challenge. The panelists addressed the need to define the challenge to the American public and find ways to attract the appropriate personnel to address them. Wibben's remarks focused on making security the fourth pillar of acquisition, articulating the threat to industry and others, and the need for increased counterintelligence resources. Several of the student questions focused on the use of artificial intelligence (AI) and how to possibly develop an AI bench to draw from. (Courtesy photo)

COACHING HELPS EMPLOYEES EXPLORE OPPORTUNITIES, IMPROVE LEADERSHIP SKILLS

by Beth Alber
Office of Public and Legislative Affairs



Over the past decade, the federal government has recognized the value of coaching in maximizing an employee's potential. The Office of Personnel Management views coaching as a tool to help employees become better performers and develop leadership skills. Coaching services can be conducted as stand-alone, or integrated as a part of training and development programs within an organization, frequently coupled with mentoring.

Within DSS, three individuals have taken the necessary steps to become coaches.

La Shawn Kelley, former chief of the Human Capital Management Office, earned the International Coaching Federation (ICF) Associate Certified Coach credential. Kelley also earned the Federal Internal Coach Training Program (FICTP) credential, along with Denise Arel, Financial Management, and Tara Petersen, Office of Acquisitions.

"As a human capital professional, I am intimately aware that the core of any organization is its workplace culture, and I am continually seeking opportunities to promote collaboration and self-sufficiency in the workplace," Kelley said. "When I came across this training opportunity, I was a little reluctant to engage, as I viewed coaching as another form of mentoring. However, when I further explored the concept of coaching, I realized that coaching and mentoring were two very different leadership techniques that can yield completely different results."

"My personal thought is that we all encounter hurdles or road blocks periodically that keep us from reaching our goals, but having access to a coach can be a great resource to tackle those challenges so that DSS personnel can more effectively achieve their objectives," said Petersen.

"I want to coach employees to take ownership in the organization's goals and be the driving force who inspires individuals or teams to imagine, innovate, and create the next big thing that benefits the agency and the federal workplace," said Arel.

FEDERAL INTERNAL COACH TRAINING PROGRAM

While the role of a coach is to help employees improve themselves, the two certification programs are slightly different. The FICTP credential, which is sponsored by the Office of Personnel Management and certified by the International Coaching Federation, is designed to prepare participants to educate, promote, and foster a coaching culture within the federal government. The FICTP is a 7-month program that requires the full participation and engagement of each participant. Completing the mandatory certification requirement involves attending 11 days of in-person training; participating in virtual training sessions; both coaching individuals and being coached; writing a reflection paper; and completing an oral examination to demonstrate learned coaching skills. Additionally, once an individual earns the FICTP, they must annually re-certify their credential.

"I applied for the FICTP because I wanted to develop coaching skills to enhance my leadership and organizational performance during a time of significant change," said Petersen, noting the future expansion of the DSS mission to include background investigations. "What I like about coaching is the use of questioning to help someone examine their own thoughts and drivers when confronted with challenges, and how that process helps them arrive at solutions of their own making."

"I pursued the FICTP because I am genuinely interested in helping my colleagues," said Arel. "I believe in partnering with employees to encourage, guide, and support their personal and professional development." said Arel.

INTERNATIONAL COACHING FEDERATION (ICF) ASSOCIATE CERTIFIED COACH

The ICF provides independent certification for professional coaches and coach training programs. To qualify for an Associate Certified Coach through the ICF, there are three application paths to choose from.

- Successfully complete an entire ICF Accredited Coach Training Program; completion of the FICTP meets this requirement.
- Complete a minimum of 100 hours of coaching experience with a minimum of eight people.
- Complete and successfully pass the Coach Knowledge Assessment, a 155 question exam.

Kelley chose to further her coaching knowledge and after achieving the FICTP, worked to attain the second certification.

"After completing the FICTP, I was eager to advance my coaching credentials, which inspired me to become certified through the ICF," she said. "Obtaining two levels of coaching credentials deepened my level of professional growth, and I find myself seeking opportunities to engage with my colleagues and counterparts in a manner that spurs curiosity and invokes my active listening skills."

To develop a coaching relationship with any of the trained DSS coaches, employees can reach out via telephone, email, or by just striking up a dialogue. The first session typically involves setting goals, whether personal or professional, in agreement with the coach.

"Each coaching session then addresses a specific challenge or problem the employee wishes to address in the context of moving toward the established overarching goals," Petersen said, noting the goal can be anything from resolving a conflict to seeking training opportunities to overcoming barriers.

"The greater benefit I have experienced from this program is how it impacted me as a leader"

Denise Arel
Financial Management

"The coaching session is a space where the employee can feel comfortable sharing a specific challenge or problem and come away with an action plan which supports his/her personal or professional goals," Arel said. Although attaining the coaching credential was the goal, each participant experienced unexpected benefits during their pursuit of this professional development.

"The greater benefit I have experienced from this program is how it impacted me as a leader," said Petersen. "I have a new approach to problem solving, as I involve my staff more and capitalize on their perspectives and their ideas. I ask more probing questions when they bring ideas to me, to really understand what they are suggesting, to explore the possibilities. Coaching helped me approach organizational issues in a different way and I am more successful because of it."

Arel agrees, noting that attaining a coaching credential also ultimately benefits the agency.

"I see my coaching credential benefiting the agency because I can leverage my coaching style across the workforce," she said. "My long term goal is to integrate my coaching skills and techniques into daily interactions with managers and colleagues."

Petersen agreed, stating, "Assisting DSS employees in achieving their goals benefits the agency in terms of increased morale, workforce retention, and better support of the mission."

"ADAPT TO IMPLEMENTED CHANGES, EMBRACE THOSE YET TO COME" THEME OF SUPERVISORS' TRAINING

by Dahlia Thomas
Industrial Security Field Operations

Attendees Andrew Winters (left), Alexandria 1 Field Office Chief; and Joe Webb, Information Systems Security Professional Team Lead, Cypress Field Office, capture details during the conference.

"Sustaining the New Normal" was the theme of the recent Industrial Security Field Operations (IO) Directorate integrated supervisors' training event held at the Russell-Knox Building, Quantico, Va. This theme celebrated the workforce's success in adapting to the changes implemented in the agency and challenged them to embrace the changes yet to come.

More than 100 front-line supervisors from the IO, Counterintelligence, and the Industrial Security Integration and Application directorates participated in the three-day training event, along with the Center for Development of Security Excellence. The event produced a robust exchange of cross-discipline information sharing and the unveiling of several initiatives, to include the FY19 Operational Initiatives and the IO Awards Program.

In his remarks to the supervisors, DSS Director Dan Payne addressed the transfer of the background investigations mission, and the process to meld DSS and the National Background Investigations Bureau personnel into the Defense Counterintelligence and Security Agency. He said that DSS will play a key role in the area of Critical Technology Protection (CTP), and he hopes that five years from now, DSS will be the primary agency in the CTP area. Payne also said he sees the implementation of DSS in Transition (DiT) as heading in the right direction, acknowledging that some changes must be made to make the process scalable.

Payne asserted that some of the nations' biggest losses come from the Controlled Unclassified Information (CUI) arena, saying that the agency must also focus on this new mission. He indicated that DSS will help establish policy relative to how CUI is handled in the near future. He reminded supervisors of the importance and need to communicate to their workforce the critical role they play in protecting national security. Payne reassured attendees he understands the workforce is frustrated by not having all the resources they would like to do their job, but he asked that they remember what is at stake and to do their best with what they have.

Gus Greene, director of IO, recalled how far the agency has come since the transition to embrace the new risk-based methodology began. He asked attendees, to step back and think about all that DSS has done to implement DiT, noting that this new way of doing business is indeed part of the "New Normal." For example:

- Since January 2018, all cleared industry's classified information systems now follow the Risk Management Framework

Patrick Ganley, Center for Development of Security Excellence, introduces his team of employees during the supervisor's conference.

Robin Nickel, Alexandria 3 Field Office Chief, takes notes during a conference presentation.

guidance prior to receiving authorization to operate.

- DSS continues to implement DiT. During FY18, IO assisted the Change Management Office in developing a new risk-based way of conducting oversight, conducted two pilots of the methodology, trained everyone on the new methodology at two events in April 2018, and conducted over 20,000 other meaningful engagements to identify and mitigate risk.
- DSS is well on its way to transition to the Enterprise Mission Assurance Support Service (eMASS) in early 2019. DSS and industry personnel have received eMASS training, and everything is being put in place for eMASS to replace OBMS as the assessment and authorization system of record.
- DSS will continue to support the Defense Information Systems Agency with the Command Cyber Readiness Inspection mission at industry locations that connect to Secret Internet Protocol Router Network (SIPRNet).

John Massey, IO assistant deputy director for Operations, also carefully laid out the FY19 IO Initiatives. One of the most innovative is the creation of the National Access-Elsewhere Security Oversight Center, which works to mitigate risk and help DSS become more efficient by balancing the workload across field operations.

Supervisors participated in several sessions during the three days of training. These included: DiT Implementation Results and Way Ahead; cross-directorate sharing; and interpreting the Employee Relations and the Federal Employee Viewpoint Survey results. In the latter session, supervisors analyzed survey results and provided specific solutions to some of the more critical personnel issues impacting the agency.

Participants acknowledged that the FY19 Supervisors' Annual Training event was one of the best training events DSS has conducted. They left the event with a clear awareness of the new normal and equipped to embrace the coming changes.

HUNTSVILLE PROVIDES TRAINING ON TARGETED TECHNOLOGIES TO BETTER UNDERSTAND BEST METHOD OF PROTECTION

by Michael Dorsett and Deborah Drake
Huntsville Field Office

With the evolution of DSS in Transition (DiT), DSS has advanced from a checklist-based mentality to an asset-driven analysis during a security vulnerability assessment, focusing on individual targeted technologies within a cleared facility. Along with this evolution, the workforce must also evolve and acknowledge the tactics of our adversaries and understand that different technologies translate to different types of security risks. The workforce is now tasked with taking a deeper look at industry's key technologies to understand the broad range of applications of the information needing protection.

Previously, the workforce did not need to have a full understanding of specific technologies to analyze their protection through the security threat checklist. However, in recent years, DSS has come to understand that the checklist-based approach leaves gaping holes in the layers of security surrounding most identified assets. The only way around the ever-advancing threat is to provide a program security plan tailored to the protection of these assets. In this spirit, the Huntsville Field Office provided training to field personnel on several targeted technologies with science and defense applications. Most recently, Huntsville hosted a classified training session on hypersonic weapons technology for employees in the Southern Region via secure video teleconference.

The informative training was presented by subject matter experts (SME) from industry and the U.S. Army. The group of 53 training participants included industrial security representatives, information systems security professionals, counterintelligence special agents, and field office chiefs, as well as Homeland Security Investigations (HSI), and FBI special agents. In the approximately two-hour long classified session, participants were provided a no-holds-barred discussion about the use of hypersonic weapons by military forces worldwide. Experts explained the science behind their development and sustainment, the current capabilities of the U.S. military and the capabilities of several countries as understood to-date. The training ended with a question and answer session in which participants asked the SMEs to pinpoint the security measures DSS should encourage when working with hypersonic technology. This training provided attendees with a real-time threat analysis and a deeper understanding of why and how to best protect this technology, and ultimately, the warfighter.

The intent of technology-specific trainings is not to develop ISRs who are experts about any specific technology; instead, the goal is to give ISRs the tools needed to speak intelligently and ask relevant questions to determine the true effectiveness of a security program. This kind of baseline technology training is key to DiT and will allow ISRs to provide an increasingly better security outlook to industry. DSS has a strong relationship with both industry and other government partners, thus, the Huntsville Field Office hopes to continue building local partnerships and requesting training on key technologies for the betterment of our contribution to national security.

An artist's conception of the X-43A Hypersonic Experimental Vehicle, or "Hyper-X" in flight.
Credits: NASA

Conference attendees address discuss various threats faced in academia during a workshop.

SECURITY CONFERENCE INFORMS ACADEMIC COMMUNITY OF EMERGING THREATS, EFFECTIVE MITIGATION STRATEGIES

by Kevin R. Gamache
Chief Research Security Officer
Texas A&M University System

Editor's Note: The following article is a first person account of the Texas A&M University Academic Security Conference. The article reflects the author's thoughts and opinions.

The 2019 Academic Security Conference, hosted by the Texas A&M University System, represents a successful incorporation of security, cultural and operational objectives. During the conference, DSS personnel introduced DSS in Transition (DiT) to U.S. colleges and universities as a functioning change from auditing compliance to an intelligence-led, asset-focused, threat-driven approach to security oversight.

Educational institutions and government security agencies received valuable information on emerging threats and participated in a workshop designed to implement effective practices that mitigate threats to cleared universities and help stem the loss of the U.S. classified and proprietary information. Moreover, DSS informed the academic community about critical acquisition programs and methods to build support for those universities performing on technologies requiring enhanced protection.

Security and compliance personnel from more than 60 universities across the United States gathered in College Station, Texas, in February 2019, to learn and collaborate on ways to improve their organizations' industrial security programs. The A&M system established this forum in 2017 to allow facility security officers from the academic community to come together to discuss the unique challenges of maintaining a robust security program in an open academic environment. The conference agenda featured a number of national counterintelligence leaders who shared their unique perspective of the threat the United States is facing today.

DSS Director Dan Payne emphasized that academia is a prime target for nation states. More than 1.4 million foreign students are enrolled in U.S. colleges and universities, and over 300,000 of these scholars are from China.

FBI Executive Assistant Director for National Security Jay Tabb, Jr., scoped the magnitude of the challenge this nation's academic institutions are facing. The People's Republic of China's Five-Year Plan-focused goals are to own 40 percent of the advanced technology in the world by the year 2020; and to own 70 percent of the world's advanced technology by the year 2025.

One of the primary means for achieving these goals is through China's 'brain gain' activities, such as the foreign talent recruitment programs.

National Counterintelligence and Security Center Director William Evanina told the attendees that the U.S. Government estimates $500 billion in intellectual property loss occurs every year in the United States. He went on to say it is "incomprehensible" to understand the impact and totality of our intellectual property losses in the United States.

Kevin Gamache, Chief Research Security Officer, Texas A&M University System, provides opening remarks to conference attendees.

While the conference was focused primarily on sharing threat information, the attendees also engaged in development of procedures that can be used across the academic security and compliance community to address the significant threats they face. One conference workshop resulted in identification and promulgation of more than 60 best practices for vetting incoming visiting scholars. These best practices can be used by individual universities to make risk-based decisions for which visiting scholars should be allowed to do collaborative research with their respective institutions.

The conference was extremely well-received by the attendees who remarked that the event "gets better each year." One attendee noted, "It's the one conference I always look forward to each year" and "I thought this year's conference was the best yet and left me with plenty to bring home to brief my leadership and university faculty."

(Note: Demetric Tucker, San Antonio Field Office, also contributed to this article.)

COLLABORATIVE RELATIONSHIP CORNERSTONE OF

by L. Darnell Carlisle
Industrial Security Field Operations

There is a small subset of facilities in the National Industrial Security Program (NISP) working under a reciprocal relationship, where the private-sector processes to operate under the supervision of a federal installation commander. Government Owned, Contractor Operated (GOCO) facilities are locations owned by federal agencies and operated in whole or in part by private contractors. Within the Department of Defense (DoD), GOCOs are usually located on military installations. Under this concept, DoD turns over an entire building or operating location, including all of the contents, to a contractor. This alliance allows each partner to perform duties for which it is uniquely suited: DoD establishes the mission areas and the private sector implements the missions using best business practices. Currently, DoD has over 60 GOCO facilities, which demonstrates continued collaboration between government and private industry.

HISTORY

According to Department of the Army Pamphlet 27-100-131 Military Law Review (1991), GOCOs were predominantly weapons facilities that acted as the primary supplier of the nation's military munitions shortly after the outbreak of World War II. World War I production and shipments to Great Britain had depleted total reserves of small arms munition in the United States, leaving the country with a deterioration of its stockpiles. The remedy to this situation was the creation of GOCOs in the munitions industry and, in July 1940, the Ordnance Department signed its first GOCO contract to manufacture smokeless powder at what later was called the "Indiana Ordnance Works." By 1944, 72 GOCO facilities were operating, 12 of which were devoted primarily to the manufacture of small arms ammunition. From these GOCO plants, a virtual avalanche of munitions flowed. By the close of the war, over 41 billion rounds of small arms ammunition and one billion rounds of larger munitions were produced. The use of civilian operating facilities on military installations was ultimately successful during World War II. Over time, GOCOs have transitioned from producing mostly ammunition to supplying products in numerous technology areas, ranging from aerospace, combat, and marine systems to advanced research and development, federally funded research and development centers, and laboratories engaged in national defense research and production activities.

Just like other facilities in the NISP, GOCOs must obtain and maintain a facility clearance (FCL) before accessing classified material. Also, GOCOs are required to adhere to applicable NISP Operating Manual (NISPOM) requirements, such as the work areas of GOCO facilities must be segregated from the main base operations. The GOCO must maintain management control over its operations and be a long term operation of a year or more. Additionally, the physical security procedures of a GOCO must be separate from the sponsoring activity.

Once it is determined that a facility is a GOCO and an FCL is required, the respective installation commander will endorse an FCL sponsorship request and submit it to DSS through standard FCL sponsorship procedures. They must also determine who will assume responsibility for all aspects of security oversight: the installation commander or DSS, the responsibility can't be divided.

When DSS assumes cognizance of a GOCO facility, it executes its mission as it would any other cleared facility that it oversees.

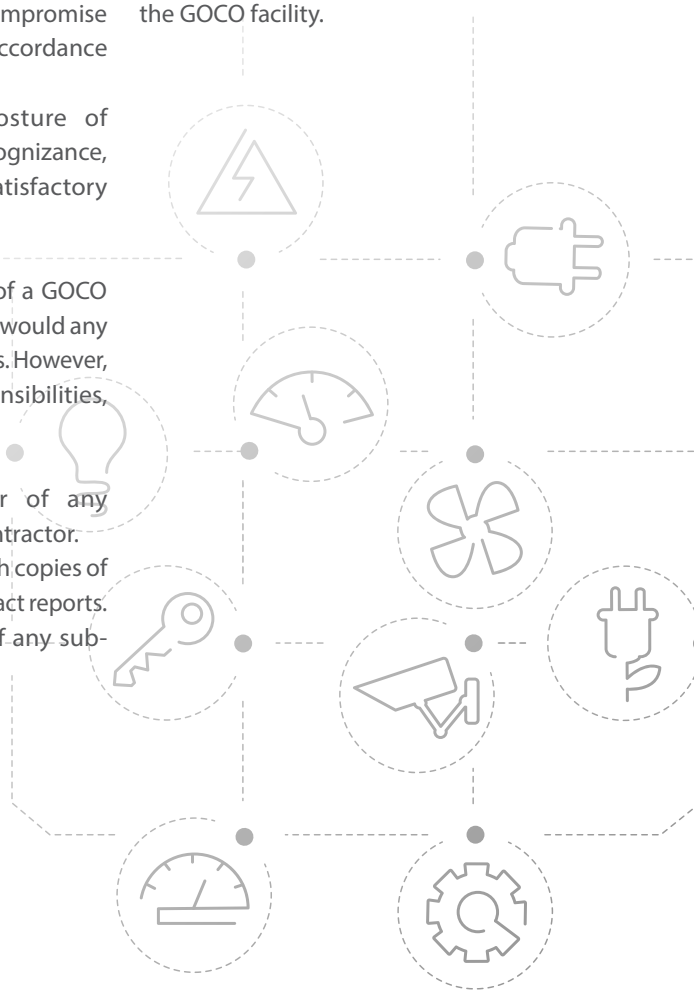
If the commander maintains oversight, there are a number of activities that must be performed, to include:

- Ensuring their industrial security personnel complete the appropriate security education and training.
- Notifying DSS of any changes affecting the FCL (e.g., change of ownership, change of key management personnel, change in foreign ownership, control or influence factors, change in safeguarding capability, or any other factors in referenced above).
- Approving safeguarding capabilities, as needed, and provide notice to DSS of the initial approval and immediate notice of any changes to that safeguarding capability.
- Ensuring that the contractor reports suspicious contacts and any incidents which involve actual, probable or possible espionage, sabotage, terrorism, subversive activity, or the loss, compromise, or suspected compromise of classified information in accordance with the NISPOM.
- Assessing the security posture of GOCO facilities under their cognizance, and notifying DSS of sub-satisfactory security ratings.

When DSS assumes cognizance of a GOCO facility, it executes its mission as it would any other cleared facility that it oversees. However, there are some additional responsibilities, including (but not limited to):

- Notifying the commander of any significant changes to the contractor.
- Providing the commander with copies of any submitted suspicious contact reports.
- Notifying the commander of any sub-satisfactory security ratings.

Additionally, DSS provides support to industry, other government, and DSS personnel to assist with identifying whether a contractor's operations meet the GOCO criteria. This includes providing an annual list of all known cleared GOCO facilities to the industrial security representatives for each of the military services. Each year, the military services must confirm whether DSS or the commander retains security cognizance of the GOCO facility.



DSS ACCESS

DEFENSE SECURITY SERVICE | WWW.DSS.MIL