Official Magazine of the Defense Security Service | **Volume 8, Issue 1**

THIS ISSUE

Outreach, integration key factors in executing successful security reviews

DSS ACCESS

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 |
Marc Pulliam

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.

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

All pictures are DoD photos, unless otherwise identified.

COVER STORY: OUTREACH, INTEGRATION KEY FACTORS IN EXECUTING SUCCESSFUL SECURITY REVIEWS

INSIDE

DSS IN TRANSITION

AROUND THE REGIONS

ASK THE LEADERSHIP

From the Director

As anyone who reads ACCESS knows, about 18 months ago, DSS embarked on a new methodology called DSS in Transition, representing a fundamental shift in how we oversee contractors cleared under the National Industrial Security Program. In short, we have shifted from schedule-driven compliance to an intelligence-led, asset-focused, and threat-driven approach that will enable DSS to provide tailored industrial security oversight. As I told our field operations supervisors in January, as we move into Phase IV of implementing DSS in Transition, I am not surprised at what we have been learning along this journey. Some engagements have gone well, and some haven't. In every phase, our goal has been to apply the lessons from each engagement to refine the process as we move forward.

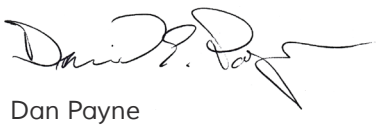
Equally important is for each field representative, regardless of discipline, to develop a risk management mindset. Each person must understand the acquisition process, use interview skills to elicit information, and use critical thinking skills to understand what's behind the processes we follow. In short, we must all become learned security professionals, not NISPOM experts.

I am pleased to see the articles in this issue giving firsthand accounts of how field personnel have adopted and internalized DSS in Transition. It's one thing for senior leaders to articulate a vision, but quite another for the experts in the field to share their experiences and perspective in actually implementing it.

I'm also excited about the outreach DSS is doing through the Air Force Lifecycle Management Center. This is a key step in our goal to protect critical technologies by integrating security and intelligence into the acquisition lifecycle. By embedding DSS expertise with acquisition and contracting activities, the Department will be much better positioned to identify and mitigate risks to technologies and programs at the earliest stages.

I concluded my remarks to the field leadership in January by emphasizing that we will continue to make adjustments to DSS in Transition. But we will not go back. I think after you read this issue, you will agree with me.

Thank you for all you do for our national security.



Dan Payne
Director

Planning, communication, integration key factors in conducting security review

Editor's Note: *In December 2018, the DSS Cypress Field Office briefed Kari Bingen, Deputy Under Secretary of Defense for Intelligence, on the DSS security reviews of cleared contractor facilities supporting the Army's Assured Positioning, Navigation, and Timing Enhanced Protection Pilot. The briefing included a discussion on the outcome of the reviews as an example of the DSS in Transition (DiT) methodology and how these reviews illustrate the way DSS is using an intelligence-led, asset-focused, threat-driven approach to protect critical technologies as part of its industrial security oversight mission. The article below explains the steps taken to ensure a successful review.*

by April Rodriguez-Plott
Cypress Field Office

As part of the DSS shift from compliance-based oversight to a more risk-based approach, the security review model has evolved to better address risk at cleared industry, especially at those facilities supporting critical technologies. In October 2018, a Cypress Field Office team consisting of Team Lead April Rodriguez-Plott; Industrial Security Representative (ISR) Miranda Johnson; Information Systems Security Professional (ISSP) Peter Hutton, and Counterintelligence Special Agents (CISAs) Marwan Binni and Glenn Hawkins conducted a security review at a cleared contractor facility supporting the U.S. Army's Assured Positioning, Navigation, and Timing (APNT) Enhanced Protection Pilot.

Adversarial threats are increasing rapidly and outpacing current GPS-reliant capabilities, which is why developing solutions to improve signal accuracy and anti-jamming capabilities for the protection of the warfighter is of critical importance. The focus of the review was on the Pseudolite Program. Described as "pseudo-satellites," Pseudolites broadcast a GPS-like signal for use in GPS denied or challenged environments.

Jennifer Gabeler, Industrial Security Integration and Application subject matter expert (SME), kicked off the effort by briefing field personnel on Army APNT programs, identifying the critical functions of the Army APNT technologies, critical components, and the threat to the APNT space. Although this was a starting place, the effort would require a greater level of engagement with the facility to identify assets and understand the technology, phases of development, and supply chain operations.

DSS engagement with industry early on in the process to inform the cleared contractor's security team and their leadership about the APNT Enhanced Protection Pilot was vital. Early communication helped set expectations and milestones for asset identification, developing a security baseline, and creating a technology map. During the first meeting, the company's leadership understood the need to engage their workforce, specifically their SMEs and program managers to work with the facility security officer (FSO) and DSS to identify critical assets that would make up the security baseline. Engaging with the onsite technical experts to identify critical assets and facilitate understanding of the Pseudolite program allowed the DSS team to gain more insight into what is critical to protect and why.

Because the APNT initiative was the first of its kind, it required coordination between DSS and the Army Protection Office, as well as the Army Program Office and Army 902nd Military Intelligence Group. There were four main lines of communication: DSS internal cross communication, DSS external engagement with the contractor, DSS external engagement with Army Program Protection Office and DSS external engagement with Army 902nd. In this case, the government customer was accessible and motivated to engage with field office personnel. The DSS team reached out to the Army 902nd, briefed them on the security review model, and asked them to join as team members. This allowed DSS to better identify areas of interest to the Army 902nd and how to incorporate them into the review. For example, the security review used for this effort is heavily reliant on interviews, and through those interactions it was discovered that the 902nd had an interest in briefing facility personnel who attend field testing. The review

offered the opportunity to connect 902nd to the right personnel while simultaneously allowing DSS CISAs to partner with their CI counterparts. This assisted the team with covering down on interviews with SMEs during the limited time at the facility.

During the security baseline meeting with the FSO and engineering team, members of the team walked through the development of the deliverable, thereby associating the listed assets with the various phases of development. There were over 90 items on the security baseline, which required input from the program office on how to scale the effort to focus on the areas of concern to the customer. DSS held another meeting with the program office to validate the security baseline and confirm the team was on the right track. The program office provided their primary areas of concern and a series of questions related to each area of focus to assist the team. From there, the team and the FSO identified and scheduled interviewees prior to the review to include procurement professionals, quality assurance, the counterfeit program lead, and others that were specific to the Army's areas of concern.

Each DSS discipline provided valuable input and a different perspective in the planning process and during the execution of the review. The CISAs developed and briefed the methods of contact/methods of operation matrix and a company-specific matrix, and used it during the interview process to educate the company's personnel of avenues of potential exploitation relevant to their duties. The ISSPs captured the protection of controlled unclassified information at the facility, assisted with the line of questioning, and covered the traditional systems review. The ISRs engaged every SME identified relevant to the primary areas of concern and focused on how the assets moved through the facility while covering traditional National Industrial Security Program Operating Manual elements.

Government stakeholder engagement is necessary to a successful outcome and to understand the security challenges of the APNT space. Ongoing communication in the planning process for the security review allowed for increased focus on areas of concern which led to several recommendations related to specific assets. From this experience, the DSS team found that focused security reviews to enhance protection of critical technologies require more time, technical understanding, and threat integration leading to a cross-discipline approach. Planning, communication, outreach, and integration were key factors in executing these security reviews. Overall, the joint effort within DSS and with external stakeholders strengthened oversight, engagement, and the execution of the security reviews to better protect critical technology.

Aligning security to the speed of acquisitions

DSS, Air Force Lifecycle Management Center establish a partnership to achieve that goal

by Tracheta Irons
Industrial Security Integration and Application

The Industrial Security Integration and Application (ISIA) Directorate is in the early stages of embedding a DSS Risk Integration Officer (RIO) with the Air Force Lifecycle Management Center (AFLMC) Information Protection Office, Wright-Patterson Air Force Base (WPAFB), Ohio. By deploying a RIO forward with the capabilities' requirement owners, DSS will become integrated into the intelligence and security support cycle sooner, and throughout technology lifecycles.

This pilot initiative is the first of several designed to create a governance structure to operationalize critical technology protection. The RIO position was developed in early 2016 to open more effective communication channels with the government acquisition community, and better integrate their expertise into DSS efforts to provide security oversight for an increasingly complex arena of continuously evolving technologies in cleared industry. In 2017, DSS in Transition (DiT) moved the enterprise from a schedule-driven, compliance-based model of oversight to one that is intelligence-led, asset-focused, and threat-driven. The RIO will be a member of an AFLMC cross-functional team integrating DSS processes, sharing DSS reporting, and representing DSS equities to mature DiT to the future of acquisition.

"Embedding DSS assets with military departments and rapid acquisition initiatives unifies DoD efforts to protect critical technology by integrating security and intelligence when risk is assumed in acquisition and contracting activities," said Fred Gortler, director of ISIA. "The initiative with the Air Force culminates a two-year investment to develop enterprise risk assessments and tailored security plans collaboratively with DoD government contracting activities (GCAs)."

As discovered during the initial phases of this new approach, the acquisition ecosystem is complex and the landscape is vast. The result for DSS is prohibitively labor intensive efforts to "pull" requisite datasets. Partnering with government stakeholders matures the DiT methodology into a more scalable and repeatable operation by "pushing" identification and prioritization of assets deemed critical to national security for oversight. Additionally, DoD is in the midst of sweeping acquisition reform designed to move faster by adopting use of other transaction authority which will have a significant impact on prototyping, research and production. Embedding a RIO with the military during this transformative period enables DSS to mature DiT at the speed of relevance.

The AFLMC is one of six Air Force Materiel Command centers and is the Air Force's single center responsible for total life cycle management for aircraft, engines, munitions and electronic systems. The AFLMC was the clear front runner for the first RIO embed, as it provides access to, and partnerships with, tenant organizations and functional center managers including program executive officers, engineering and technical subject matter experts. In addition, the location provides direct access to other key stakeholders such as the National Air and Space Intelligence Center, Air Force Materiel Command, the Air Force Research Laboratory, and the Air Force Institute of Technology.

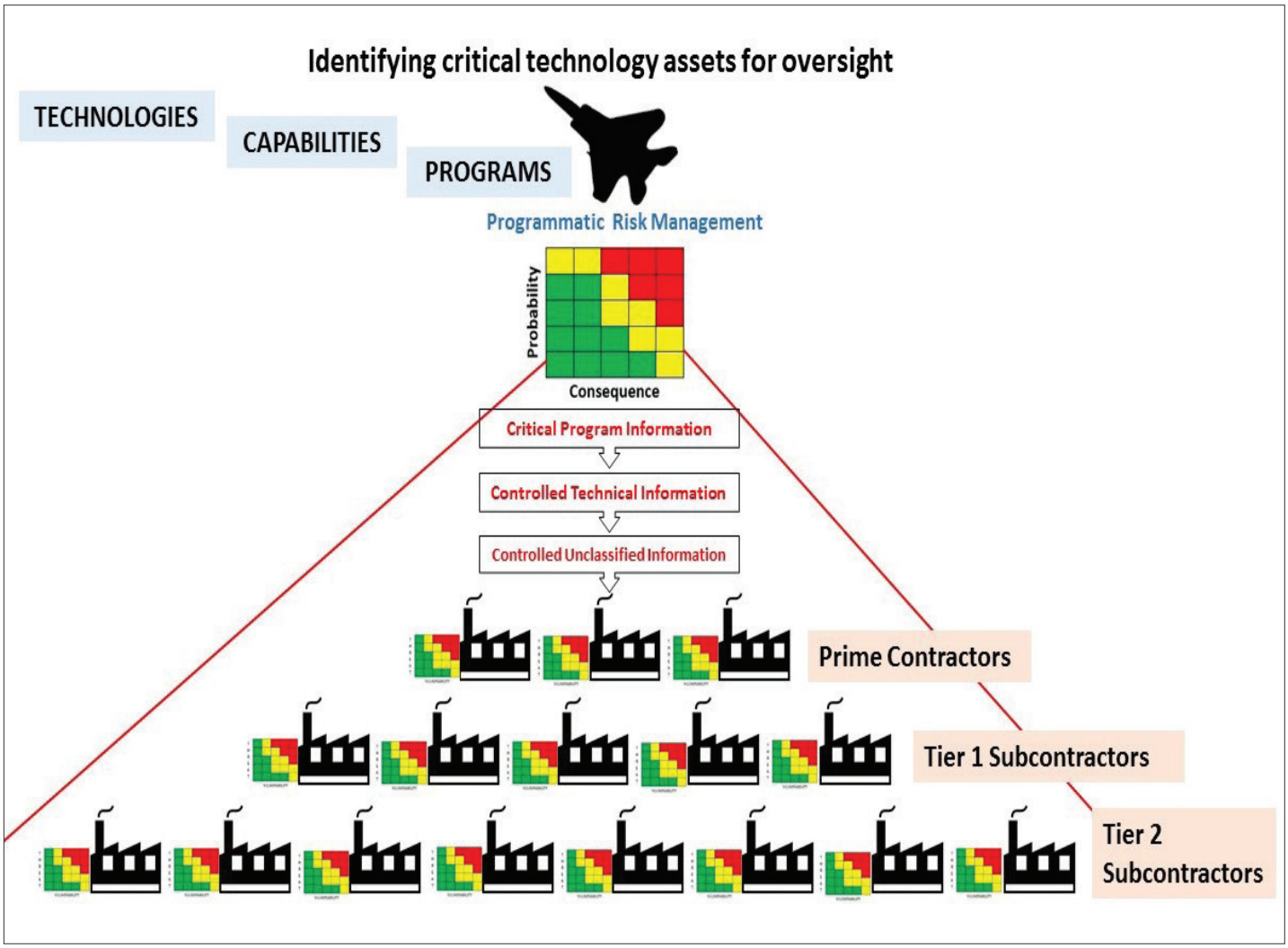
Gortler expressed confidence that the initiative with the AFLMC would enable the RIO capability to shift to a much higher operational tempo. "The execution of this initiative demonstrates the RIO role is essential in building partnerships with GCAs to protect critical technology," he noted.

Efforts are underway to create an integrated governance structure to deliver a holistic approach to critical technology protection. The concept is to create a baseline framework (see figure below) which identifies what is critical thus enabling collaborative, tailored mitigation, oversight and protection. To operationalize data sharing, the goal is to integrate community of effort processes incorporating requirements for decision makers. Baseline criteria include identifying the military's priorities, such as critical program information (CPI), and critical components, and to align CPI to contracts and DD254s to determine where CPI is resident in the defense industrial base (DIB). Mapping the CPI supply chain to the DIB is foundational to intelligence and informing government stakeholder risk management.

Without understanding what and where critical components reside, efforts made to apply oversight and risk management are ineffective and waste precious resources. Decomposing the system and overlaying components to the DIB allows an integrated security and intelligence community focus for collection, reporting, and production.

Delivering cutting edge capabilities to the warfighter continues to be a complex and multifaceted endeavor with interdependent stakeholders and missions. In the context of globalization, rapidly evolving technologies, and emerging threats a comprehensive response is essential. The National Defense Strategy and National Defense Authorization Act dictate that government stakeholders better protect the nation's investments. The challenge becomes how to mature the DiT methodology to the speed of relevance.

Long-term, DSS plans to embed a RIO at pivotal acquisition centers across the military to promote horizontal protection across government stakeholders, oversight and protection process integration, coordinate on risk management decisions, and build more effective communications between DSS and the acquisition community.



Completing the shift to an asset-focused mentality

Editor's Note: *The following reflects the thoughts and opinions of the author on the need to adopt an asset-focused mentality in relation to industrial security.*

by Misty L. Crabtree
Morrisville Resident Office

This past year, the Defense Security Service (DSS) began shifting from a compliance-based approach of conducting industrial security oversight to an intelligence-led, asset-focused and threat-driven methodology. As one of the architects of this methodology, I have briefed hundreds of internal and external stakeholders on why DSS is changing its approach to industrial security oversight, how DSS is changing, and what DSS is doing to implement this monumental change. As part of these briefings, I share my personal journey of transitioning from a compliance-based mentality to one focused on technology and asset life-cycles.

For more than 18 years, I worked with military, government, and cleared industry to ensure U.S. and foreign classified information was adequately protected. Prior to joining DSS as an industrial security representative (ISR), I spent four years on active duty in the United States Navy working as an information systems security professional and the next nine years working as an industrial security professional for several cleared contractor facilities.

EXCEEDING COMPLIANCE STANDARDS

During my time in industry, the security programs I managed exceeded compliance standards, resulting in commendable and superior ratings. I also founded and led a consulting business unit to assist other cleared contractors with enhancing their security programs and provided mentorship to hundreds of security personnel as the chapter chair for a professional security organization. I mention this not to boast about my experiences or accomplishments, but to lay the groundwork for why my "ah-ha" moment had such a profound impact on me.

I joined DSS as a rookie ISR more than five years ago accountable for conducting oversight actions for many cleared contractor facilities. It is my responsibility to assess cleared contractor compliance with the National Industrial Security Program Operating Manual (NISPOM), identify areas of non-compliance, and rate their security programs using a calculation matrix. During this time I have awarded several commendable and even superior ratings to cleared contractors based on their NISPOM-centered programs. Some of these contractors were nominated for the Cogswell award – one of the highest honors in the industrial security community.

DSS IN TRANSITION

In January 2017, I began participating in the DSS in Transition effort as a member of an integrated process team charged with conceptualizing one component of the new risk-based approach to industrial security oversight. Later that year, I was named a member of the methodology development team which would compile and release an integrated concept of operations covering all aspects of the methodology.

As part of this assignment, I learned the significant foreign intelligence threat the United States is facing. Our adversaries are stealing our information and technology using multiple and varying methods of approach, and are then using the stolen information and technology to upgrade their military capabilities and compete against us. In the past, DSS used the NISPOM to guide industrial security oversight actions. As a static policy manual, the NISPOM doesn't take into account what information and technology requires the most protection, address the ever-changing methods of contact and operation used by our adversaries, or consider the inherent vulnerabilities associated with business processes and the supply chain. Furthermore, our adversaries have full access to the NISPOM which provides them an inside look into the minimum security controls implemented across industry. Because of this, coupled

with the unprecedented threat to our national security information and technology, DSS concluded that maintaining the status quo was simply no longer an option. The "why" DSS was changing its approach was clear; however, the "how" was still to be seen.

NEW METHODOLOGY

Over the next several months, the new methodology began to take form. Although fluid, the foundational elements remained solid: prioritize technology and facilities using national security information, establish a security baseline consisting of the contractor's national security assets and implemented security controls, prepare for and conduct a comprehensive security review using threat information to identify gaps in implemented security controls, establish a tailored security plan, and continuously monitor the established plan. Developing and refining the concept of operations for each aspect of the methodology involved multiple weeks of collaboration with internal and external stakeholders. The friendly debates and practical exercises for the security review components changed my way of thinking about critical technology protection.

Until this point, security reviews primarily focused on ensuring classified information was safeguarded from loss, compromise, or harm. In spite of this, our nation's most critical technology and information is still being stolen and used against us. In order to assist contractors with delivering uncompromised products, DSS would need to expand its security review focus to include the full life-cycles of our nation's most critical assets. DSS began testing the concept by identifying national security assets related to a prioritized technology list, researching the threat vectors associated with those assets, then walking each asset through its lifecycle to ascertain if it was susceptible to loss, compromise, or harm prior to receipt, during the design or development phases, or upon delivery.

The results of these tests were eye opening. Vulnerabilities not previously noted during traditional security reviews were identified; vulnerabilities which could help adversaries collect key pieces of data regarding critical technology and information that could then be used against us. DSS learned more about the true security posture of these contractor locations during the visit than had been known in the several years prior to the comprehensive security review. Although the methodology was still being refined, its successful approach got me thinking about my personal mentality toward security and critical technology protection that ultimately led to my reflective "ah-ha" moment.

MY "AH-HA" MOMENT

During my career I prided myself on being a leader in the industrial security community. But I began to wonder if my compliance-focused tunnel mentality had prevented me from being an effective security professional. It is true that the security programs I managed throughout the years were absolutely compliant with NISPOM requirements; yet, I couldn't help but question if critical technology and information – either in my possession or at my assigned contractor sites – was protected throughout the lifecycles to prevent loss, compromise, or harm to those assets. Unfortunately, I can't definitively say it was.

Then it hit me. I was unable to adequately protect critical technology and information within my facility or at my assigned contractor facilities without understanding which national security assets required the most protection. I couldn't sufficiently identify gaps in implemented security controls without knowing the threat vectors associated with each asset. Nor was I able to ensure technology and information was delivered uncompromised by focusing solely on the classified components. This realization was humbling but critical to my growth as a leader in the security community.

Although I met full expectation for my positions it is clear to me now that those expectations are outdated and need to be more robust to meet the threat we are encountering. Just like many of you, I was taught to be an administrative compliance officer focused on NISPOM requirements. I served that role well and received high ratings for my effort. Now I know that an effective security program goes well beyond superior ratings based entirely on compliance. As security professionals, we must all become more operationally minded and shift from a compliance-based approach to a technology and asset-focused mentality. It's the best way to ensure our nation's most critical technology and information is delivered uncompromised.

Wisdom, critical thinking vital to success of DSS in Transition

Editor's Note: *The following reflects the thoughts and opinions of the author on the value of wisdom in the implementation of DSS in Transition.*

by Dave Bauer
Western Region

"In the past few years, wisdom has been put under the research microscope and found to be a distinct, measurable and precious human quality, one that is vitally important and for which there are no substitutes." This insightful quote, by Brookings Institute Fellow Jonathan Rauch, appeared in a May 2018 *The Globe and Mail* article, "A word to the wise: Why wisdom might be ripe for rediscovery." Why is developing wisdom important for DSS? From my perspective, wisdom and critical thinking are essential to the success of DSS in Transition (DiT), and the future of all current mission sets as well as those anticipated for DSS.

Most definitions of wisdom include statements about a person's ability to use your knowledge and experience to make good decisions and judgments. I prefer the quote in the Wisdom article by Dr. Monika Ardelt who said, "Wisdom is realized knowledge, it transforms the individual." The article explores the traits common in the flourishment of wisdom, to include "compassion and concern for the common good; pragmatic knowledge of life and the application of pragmatic knowledge to resolve personal and social problems; an ability to cope with ambiguity and uncertainty and to see multiple points of view; emotional stability; and a capacity for reflection and for dispassionate self-understanding." I am convinced these same traits are essential to the future of the new DSS, implementation of DiT, and our goal of delivering uncompromised technology to the warfighter.

As Dan Payne, the DSS director has mentioned several times, DiT will shift more and more responsibility to the field, to the field office and to the individual industrial security representative (ISR), counterintelligence special agent, and information systems security professional. Our collective challenge is to develop a shared, corporate wisdom to better focus a consistent effort on protecting our national security. It is easier to read a manual and tell someone they must comply with it than it is to assess, think, and develop the appropriate solution within the framework of the DSS mission and National Industrial Security Program (NISP). Wisdom is a deeper understanding of the purpose behind the guidance, and applying your knowledge and experience to make a judgment on how best to protect national security.

As we continue on the journey of intelligence-led, asset-driven, threat-focused engagements, DSS will need to create a culture that values critical thinking and seeks to develop wisdom within the work force. Here are some suggestions and thoughts to speed us along on the way.

- **Experienced DSS employees wanted!** *("The mind once enlightened cannot again become dark," Thomas Paine)*. Some more seasoned DSS employees may wonder, do I have anything to contribute in this new DiT strategy? Yes! DSS needs your knowledge and experience, which contributed to you transforming yourself into an industrial security and national security professional. Your countless hours of engagement with cleared industry, thousands of interviews, and conversations about issues that go to the heart of protecting national security, and your efforts in developing productive relationships with your industry counterparts can't be replaced. Yes, DiT is a significant change, but the many unique experiences and sharpened skills our most experienced employees possess are essential for DiT to wisely proceed.

- **Compliance and partnership** *("Alone we can do so little; together we can do so much," Helen Keller)*. A few within DSS might think, compliance or partnership. I am convinced when we shift our principles to focus discussions centered on risk and national security, we raise the criticality of the discussion and better serve the

warfighter and the nation. Then, the National Industrial Security Program Operating Manual (NISPOM) becomes a tool and the higher calling of national security becomes the guide, not meeting rigid and often outdated guidelines. To move DSS and industry in this direction, we must begin and end each engagement with the true risk picture. Not an embellished picture to support our demands but an accurate depiction of what we know, what we don't know, and what we think. For those rare occasions when DSS is unable to convince industry of the threatened national security interests, DSS's regulatory and compliance authority, along with our official relationship with the government customers, can be leveraged to gain the appropriate decision. I believe the strength of DSS and DiT is raising effective protection through the education of industry on the threat and risk to their technology and brand.

- **Raise the discussion** *("The mind, once stretched by a new idea, never returns to its original dimensions," Ralph Waldo Emerson)*. I attend annual NCMS and NDIA conferences where government and industry frequently discuss the inconsistencies of the field. Industry is correct, we are inconsistent within each office, within each region, and within each discipline. But isn't that the nature of 400 different professionals, with different experiences in different facilities trying to execute a large mission? Each DSS representative has different relationships, different interests, different experiences, and each of these factors contribute to their approach and assessment of a facility. I suggest the more important question, are we consistent in centering the discussion on risk and threat? By making that the objective of the engagement, we gain greater flexibility to pursue the spirit of the DSS mission statement and the NISP. So, if you find yourself in a conversation with an industry partner, try asking "where is the national security concern?" If you can't come up with an answer, then maybe it's a point not worth considering.

- **Move now** *("The best time to plant a tree was 20 years ago. The second best time is now," Chinese proverb)*. We will not get better at developing our skills and our people until we move decisively toward the DSS director's vision. Consider the analogy of learning to drive a car which seemed incredibly complex. How do I keep the car on the road, check my mirrors, anticipate what is ahead, and monitor my gauges all at the same time? Only after getting behind the wheel over and over again did I get comfortable and within a short amount of time, I was doing all those things plus rolling down the window, changing stations on the radio, or putting in an 8-track tape to listen to music. For almost everyone, DiT, the 12x13, the baseline technology mapping seemed too much, but given time, it will slow down and become easier. I know this because I have seen it within the Western Region. Many of my most skeptical ISRs are now the best at delivering tailored 12x13s, discussing technology mapping and the other aspects of DiT because they got started, tried, stumbled, and tried again. Their confidence and courage to step out, knowing it would get easier, has made all the difference in their performance, and their impact within their office and the region.

- **Continually share your experiences, successes and failures** *("Success is not final, failure is not fatal: it is the courage to continue that counts," Winston Churchill)*. I have learned a little from reading, but I have learned much more doing, watching and listening to those that have done it. Regardless of your specialty or your grade, you can be a student and a teacher to your colleagues. One of the greatest tools available to everyone is the "What Everyone Should Know" report. This simple, still developing weekly report provides DSS with a catalog of success stories that each can absorb. However helpful it is though, this report can't replace the day-to-day interactions between co-workers, lifting each other up and investing time in each other to make the other better. Our willingness to share experiences and have candid conversations about what is working and where someone is struggling strengthens us all.

During this phased approach to DiT, I hope you'll reflect on the past year and see the progress that you and your co-workers have already made toward the goals of securing our nation's crown jewels and providing uncompromised technology and capabilities to the warfighter.

A Q&A with **Timothy A. Davis**, Director of Strategic Planning and Integration

Editor's Note: *The following is the latest installment in a series of features on the DSS senior leadership team.*

Timothy A. Davis, a Defense Intelligence Senior Level, was named the director, Strategic Planning and Integration of the Defense Security Service in April 2018. In this capacity, he is responsible for overseeing the Program Integration Office, Enterprise Data Management, Director's Action Group, Strategic Management Office, and Office of Public and Legislative Affairs.

Prior to this, he served as the DoD senior advisor, Office of the Director of National Intelligence, National Insider Threat Task Force. Previously, Davis was the director, Security Policy and Oversight Division, Office of the Under Secretary of Defense for Intelligence, and served as the Security Director, Headquarters U.S. Air Force, Director of Intelligence, Surveillance, and Reconnaissance.

Davis entered the Air Force in 1971, serving as a personnel specialist, and was honorably discharged in the rank of "buck sergeant" in 1975. He was commissioned a second lieutenant in 1979 and assigned to the Air Force Office of Special Investigations (AFOSI). He held various positions within AFOSI, retiring as the AFOSI Region 3 commander, Scott AFB, Ill., in August 2007. He is the recipient of numerous military decorations, including the Legion of Merit.

Davis holds a bachelor's degree in Forensic Studies, Indiana University; a Masters of Forensic Science from The George Washington University; and a Fellowship in Forensic Pathology from the Armed Forces Institute of Pathology, Walter Reed Army Regional Medical Center. He retired, as a Fellow, from the American Academy in Forensic Sciences in 2016.

Q: Tell us about your background and what led you to this position?

I was the DoD senior advisor to the National Insider Threat Task Force, National Counterintelligence and Security Center, from April 2015 to April 2018. Prior to that I was the director, Security Policy and Oversight, Office of the Under Secretary of Defense for Intelligence. So I've been working with DSS in some capacity for almost 10 years. Based on my experience and the opportunity to stand up this new office, it seemed a natural next step. And, with all the changes coming to DSS, it's an exciting time to be here.

Q: This is a new position for DSS, what are the goals of the office?

The goals of the office reflect the stated goals of the functional mission areas of the Strategic Management Office (SMO), Program Integration Office (PIO), Office of Public and Legislative Affairs (OPLA), and the Director's Action Group (DAG). The overarching goal(s) are, in part, targeting support to our regional directors and field office chiefs, and to confirm and maintain relevance to our main mission directorates.

Q: You seem to be pulling together disparate functions into one office, SMO, PIO, OPLA, etc. What are the challenges with doing that? What success have you seen?

I think a challenge will be to bring all of the goodness being done within each of the individual offices and finding the common functional mission space(s) and initiatives to demonstrate a nexus to the Director's

Strategic Guidance. There have been a number of successes, to date, demonstrated within each area - from enhancing the governance process related to vetting and validating mission requirements and technologies; methodically defining and refining internal and external communications; publication of the Director's Strategic Guidance; and leading and/or facilitating initiatives, identified by senior leadership, for enterprise planning, engagement, reorganization and integration.

Q: You have also stood up the DAG, which is another new office. What can you tell us about that office?

The Director's Action Group was conceived by the Director, Deputy Director and Executive Director as an asset to address organizational themes aligned to strategic development; workforce readiness; organizational design and stakeholder alignment. To date the DAG has done an astonishing job in addressing and accomplishing a number of leadership directed tasks.

Q: What are the biggest programs/projects you're working on?

Right now our collective efforts relative to programs/projects, at large, are focused on and in support of the moving pieces/parts having a nexus to the pending transfer of the background investigation mission from the National Background Investigations Bureau to DSS. So for us it is the strategic planning, the internal and external communications, the validating of requirements and vetting/validating those requirements to the Integrated Lifecycle Management Framework, and appropriate engagement as needed/required for organizational design, workforce readiness and stakeholder alignment.

Q: What are the next steps for the office?

To evolve, adapt, and adopt as needed and required by senior leadership on any and all initiatives.

Q: Anything else you would like to add?

I've been blessed to have been given this opportunity to be at DSS headquarters and work with awesome professionals. It's all good.

TBM framework provides DSS with tool to run information technology more business-like

by Beth Alber
Office of Public and Legislative Affairs

In the evolution of improving information technology (IT) management, investments, and cost, industry and government, together, have created a framework called Technology Business Management (TBM). This framework provides a means of communicating IT costs and decision making through a taxonomy relatable to business partners, finance, and management decision makers. Thus, the federal government is adopting the TBM framework to more effectively manage information technology efforts and be more fiscally efficient. The framework is part of the President's Management Agenda, with an associated goal of government-wide adoption by fiscal year 2022. The DoD Chief Information Officer (CIO) has mandated the adoption of TBM across the Department by fiscal year 2020.

DSS has started the implementation of TBM with the primary goal to allow for data-driven discussions about cost, consumption and performance of IT to best support business goals. These discussions are in terms of IT services and investments with business partners, finance, and IT in order to better track spending, determine where savings can be found or the best course of action when making IT investments.

In order for DSS to begin the TBM adoption process, three DSS employees earned their TBM Executive Foundation Course certifications. This is the only course authorized by the TBM Council that governs the framework. By completing this course, each person now has the knowledge and information about the TBM framework in order to build and implement the framework within an organization and the value it has to each partner organization.

Chris Bowman and Eric Von Dibert, Office of the Chief Information Officer, earned their TBM certifications in 2018 after completing the course and passing the required exam. Vanessa Womack in the Financial Management (FM) Division has also completed the course. The certification gives official recognition by the TBM Council that the recipient has demonstrated proficient knowledge about the TBM framework.

> "Once we determine a solution, then we can start incorporating the various aspects of the TBM framework and taxonomy into the IT efforts."

"The TBM framework is a tool to run information technology in a more effective, business-like manner," Von Dibert said, noting that DSS is in the early stages of adopting TBM.

Currently, the DSS OCIO is conducting an opportunity assessment, where they will investigate and examine all available software applications used to implement TBM to determine which application would be the best solution for the agency to adopt in conjunction with FM and other business partners, said Von Dibert.

"Once we determine a solution, then we can start incorporating the various aspects of the TBM framework and taxonomy into the IT efforts," Von Dibert said, explaining that the TBM framework will help improve existing governance, policies, standards, practices, and processes in order to monitor IT investments and costs on an ongoing basis through a common language taxonomy.

Von Dibert further explained that the TBM taxonomy provides a means for program managers to group and communicate IT spending via four views – finance, IT Towers (areas of IT operations), IT services and business capability/investment. This will help everyone within the agency understand how IT resources are applied across the agency in support of the mission and the impact of respective decisions on programs.

Another aspect of TBM is that it provides insight into a variety of comparison metrics against other like organizations, which will help drive informed decisions on how effective we are operating and help determine where cost savings can be found, he noted.

OCIO initiatives

Support DSS workforce, stakeholders; respond to unprecedented challenges

The Office of the Chief Information Officer (OCIO) has a variety of technology priorities for the fiscal year which supports diverse and complex stakeholder requirements, as well as responding to unprecedented challenges, including transformation, reorganization, operations and mission support, and cyber readiness. Some of the priorities are internal, while others are initiatives that support the larger DSS stakeholder community.

"Our priorities are nested in the broader DoD priorities, which include information technology (IT) reform, and are aligned with the DSS director's fiscal year 2019 focus areas. Specifically, we are looking at ways to use IT to reduce labor and allow our personnel to focus on the substantive aspects of their jobs," said Jimmy L. Hall Jr., acting Chief Information Officer.

Initiatives supporting the DSS workforce include executing initial cloud migration, which will transition certain systems to a cloud service provider thereby providing a cost savings. Another is abiding by the DoD Information Technology Reform Initiative, which will streamline IT requirements and acquisition processes to consolidate like services. And finally a third initiative is designed to integrate people, processes, networks and supporting technologies associated with bringing the security clearance vetting mission into the DSS enterprise.

Other priorities align with DoD efforts related to information technology. Recently, the DSS public website transitioned to a web platform hosted by the Defense Media Activity, and the unclassified internal website migrated to the Defense Information Systems Agency Enterprise Portal, both of which support DoD's move toward common shared services and cloud technology.

Additionally, OCIO is overseeing the maintenance of the National Industrial Security System, the information system that replaces both the Industrial Security Facilities Database and Electronic Facility Clearance System. They are also spearheading the effort to develop the DoD Insider Threat Management and Analysis Center System of Systems, which is an insider threat collaboration system to better facilitate information sharing, analysis, and insider threat mitigation across the Department.

Ensuring security of the networks is vital to the agency's mission, and several initiatives support this effort. The OCIO is sustaining a cybersecurity posture that ensures confidentiality, integrity and availability of mission data and information systems. It is also complying with cyber workforce management guidelines by establishing enterprise-wide qualification standards for education, training, and personnel certifications for select government and contract employees who conduct information assurance functions.

A few initiatives support the Center for Development of Security Excellence to include enhancing the CDSE network and virtual student classroom environment to meet increased user and mission demand for security education, training or certification; as well as conversion of the Security Knowledge Management System to USA Learning which provides a simplified and one-stop access to high quality e-learning products, information and services.

COR program

Compliance, consistency key to success

by Cristina Dupont
Office of Acquisitions

Beginning in fiscal year 2013, the Defense Security Service (DSS) embarked on creating a Contracting Officer's Representative (COR) program that would not only be compliant with DoD direction, but also implement a DSS strategic objective to improve contractor performance. The DSS COR regulation was written in 2010 and needed to be updated, to include the DoD Contracting Officer Representative Tracking (CORT) tool. The Office of Acquisitions (AQ) had oversight of the COR program, and took the opportunity to make improvements by launching a program that provides guidance, instruction, accountability, compliance, and consistency.

DSS kicked off the program by hosting Defense Acquisition University (DAU) training in March 2013 for CORs, supervisors and potential CORs. Over 50 people were trained. The COR program continued to evolve in significant areas, such as:

- Establishment of metrics that track COR training
- Contractor Performance Assessment Reporting System (CPARS) status and completion rates along with COR annual file reviews
- Updated local policy and COR initial training process improvements
- Targeted training topics
- Continuous customer outreach, monitoring, and follow-up
- Establishment of the COR program manager position

From the beginning, compliance and consistency have been a cornerstone of the DSS COR program success. Highlights of the program success and accomplishments include:

- Establishment of local COR policy
- Use of the CORT tool
- Leadership direction and support for program development
- Development of a performance objective-specific to COR duties in the personnel performance plan of each COR
- Hands-on training workshops with groups and individuals

The Office of Acquisitions continues to emphasize customer support and engagement as key elements in building stakeholder support. The COR program manager demonstrates this by acting as a liaison between Acquisitions and directorates receiving services.

The synergy created by the COR program manager with contracting officers and DSS directorates has been commended in the two most recent Program Management Reviews (PMRs), and has resulted in several success stories:

- Reduces burden from contracting officers by facilitating contracting officer annual file reviews, which has resulted in 100 percent completion since its 2014 inception
- Ensures CPARS are completed in a timely manner, leading to an average completion of 97 percent
- Timely invoicing reduced payment interest penalties by 66 percent over the past two fiscal years
- Ensures CORs are aware of Enterprise Contractor Manpower Reporting Application reporting requirements and holds contractors accountable for reporting completion. This has allowed for the inventory of contracted services report to be compiled quickly using actual contractor reported full time equivalents.

Every step of the way, the DSS COR is equipped with the training and knowledge to be successful in

> **DSS** has been able to **adhere to the** Services Requirements Review and stick to fiscal year-end deadlines and, moving forward, will continue to track metrics on program performance.

contract oversight and management. CORs complete initial training through DAU, receive annual and refresher training based on "require reinforcement" metrics, and have clear performance objectives that set the expectations for success. CORs have the support of senior leadership and perform work in environments where they are encouraged to ask questions that will enhance their understanding of contracts. They are routinely provided assistance by the COR PM whenever requested, and are instructed to work closely with contracting officers and contracting specialists to ensure a thorough understanding of roles and responsibilities, including:

- Understanding contract terms and conditions
- Adherence to Procurement Acquisition Lead Times
- Timely submission of critical documents in the performance of their COR duties

Training provided by the COR PM also addresses the significant role played by both the DSS Financial Management and Program Integration offices in the Service Requirements Review Board process and budget execution requirements. Additionally, DSS established the "COR of the Year" award to acknowledge the significant impact a COR has in contract oversight and management. The award also provides an opportunity to acknowledge that the responsibilities and duties performed are in addition to primary duties.

Since the program was formalized in 2014, 80 DSS personnel have taken the COR training. DSS directorates have adopted a COR "bench ready" approach, with personnel completing the COR training so they are "bench ready" at any time to be appointed a COR on a contract. At DSS, there are a group of appointed CORs and in each component there are also "bench ready" CORs.

What worked?

Among the directorates and across DSS, the cumulative positive impact of leadership support for the DSS COR program has been instrumental to its success. Leadership highlighted the importance of the DSS COR program in staff meetings at all levels. That message filtered throughout the DSS staff, generating increased interest in COR training and that, in turn, led to an increase in comprehension of COR responsibilities. By establishing this framework – along with its "bench ready" philosophy -- DSS has been able to adhere to the Services Requirements Review and stick to fiscal year-end deadlines and, moving forward, will continue to track metrics on program performance.

DSS bids farewell to senior leaders

The Defense Security Service bid farewell to several senior leaders in December due to retirements.

Mark S. Allen

Allen, a Defense Intelligence Senior Level and the deputy director of the Counterintelligence Directorate, retired in a ceremony on Dec. 20, 2018.

He started his federal career at DSS in 1985, as a senior industrial security specialist. He served in various positions within DoD to include: chief, counterintelligence, Defense Threat Reduction Agency (DTRA); chief, security services, DTRA; counterintelligence program manager; and counterintelligence liaison for arms control, DSS/DTRA. He returned to DSS in November 2008.

During the ceremony, Allen was presented with the Distinguished Service Award in recognition of contributions to DSS from November 2008 through April 2019. During this period, he spearheaded a number of critical initiatives that led to improved communication within DSS, the department, cleared industry, and the federal government, enabling the identification and mitigation of risks to sensitive technologies within cleared industry. Under Allen's leadership, the CI directorate aggressively strengthened relationships between industry and interagency partners by hosting monthly secure teleconferences, a unique service offered to industry in partnership with federal law enforcement, counterintelligence, and intelligence professionals. Approximately 5,000 attendees from more than 40 secure locations nationwide participate in these sessions, which contributed to a 676 percent increase in suspicious contact reporting submitted by the cleared contractor community. These reports are foundational to all activities originating within the CI directorate and have directly contributed to more than 3,000 subjects of investigation and 775 potential sources to appropriate agencies since 2009.

DSS Director Dan Payne (right) presents a retirement plaque to Mark Allen at his retirement ceremony. *(Photograph by Hollie N. Rawl, CDSE)*

With only 3.5 percent of the department's counterintelligence resources, Allen maximized the effectiveness of every employee in the directorate, contributing significantly to the agency's continued success as a premier reporter to the Intelligence Community. Notably, DSS CI collection efforts in 2018 accounted for 26 percent of all DoD CI intelligence information reports, and 74 percent of all DoD intelligence information reports on foreign intelligence entity threats to research, development, and acquisition.

Denise D. Humphrey

Humphrey, a Defense Intelligence Senior Level and the deputy director of the Center for Development of Security Excellence, retired in a ceremony on Dec. 18, 2018.

She joined DSS in July 1998, and during that time she worked in a number of positions to include DSS Academy instructor, information security team leader, distance learning development manager, curriculum manager, and operations manager.

During the ceremony, Humphrey was presented with the Distinguished Service Award in recognition

DSS Deputy Director James Kren (left) presents a letter to Denise Humphrey, CDSE Deputy Director during her retirement ceremony. *(Photograph by Hollie N. Rawl, CDSE)*

of sustained, exemplary service from July 1998 to November 2018.

She designed, developed, and implemented the Security Professional Education Development (SPēD) certification program, the first comprehensive professional certification program within the Office of the Under Secretary of Defense for Intelligence, followed by the establishment of the DoD Security Training Council, which serves as the governance body for the SPēD certification program.

A strategic thinker, visionary, and proven leader, Humphrey was instrumental in leading CDSE into the next generation of training delivery methodology. She was singularly instrumental in the conversion of course content for instructor-led courses into foundational learning modules via eLearning, addressing an ever-evolving security training needs environment.

Michael P. Seage

Seage, a Defense Intelligence Senior Level and the director, Defense Insider Threat Management and Analysis Center (DITMAC), retired in a ceremony on Dec. 10, 2018.

He joined DSS in July 2016, after serving 30 years in the U.S. Army on active duty and in the Reserve. He began his civil service career in 1995, with the U.S. Marine Corps as a counterintelligence analyst at the Marine Corps Intelligence Activity, before returning to the U.S. Army. His last assignment with the U.S. Army as a civilian was as the chief, Insider Threat, Intelligence Oversight and CI Policy, for the Army Staff.

During the ceremony, Seage was presented the Distinguished Service Award in recognition of significant contributions to DSS from July 2016 to December 2018. During this period, Seage oversaw the insider threat mitigation efforts conducted by 43 DoD component insider threat programs across the enterprise. He ensured consistency in mitigating more than 1,500 insider threat issues reported to the DITMAC since achieving full operational capability in 2017. Through his exceptional leadership, vision, and innovative spirit, Seage led the DITMAC in establishing a viable, enduring insider threat operational capability to support the entire Department of Defense. He fostered an environment that enabled the DITMAC

DSS Deputy Director James Kren (left) presents Michael Seage with a Distinguished Service Award at his retirement ceremony.

team to build relationships, train personnel, create processes, develop product lines, and implement new technical capabilities. He oversaw the development, implementation, and adoption of the first enterprise case management and data repository system for insider threat information. Moreover, his leadership was instrumental in accelerating the incubation of the DITMAC to full operational capability and expanding the role of the DITMAC with the formal assumption of the Unauthorized Disclosure Program Management Office and establishment of the Insider Threat Enterprise Program Management Office. Seage deftly positioned the DITMAC to be seamlessly woven into the overall fabric of the new Defense Vetting Directorate's end-to-end consolidated vetting enterprise. His leadership, determination, perseverance, and dedication to mission elevated the DITMAC as a model insider threat operational capability within the federal government.

What is a DISL?

All three of the individuals who recently retired from the Defense Security Service – Mark S. Allen, Denise D. Humphrey, and Michael P. Seage – held the title of Defense Intelligence Senior Level. Employees holding the title of Defense Intelligence Senior Level, or DISL, are experts in their fields. DISL positions are technical or scientific positions, which are characterized by emphasis on functional expertise and have no more than minimal supervisory responsibilities (less than 25 percent). DISL's are recognized leaders and authorities in a specialized field or functional area, and serve as independent leaders and technical advisors.

Field office chief retires

In October 2018, Michael Stell (shown on right in photo on right), Colorado Springs Field Office chief, retired after 32 years of service to the Defense Security Service. On hand for presentations were Dave Bauer, Western Region director, and Karl Hellman (left in photo on right), National Industrial Security Program Authorizing Official. Stell began his career as a personnel security investigator in 1986, went on to serve as an industrial security representative and regional industrial security coordinator, and culminated his career as a field office chief in Pasadena, Calif., and Colorado Springs. *(Courtesy photos)*

Cybersecurity symposium explores threat awareness data, developments

by Dan Finucane
Industry Security Field Operations

For the second year, experts in the field of cybersecurity gathered to present vital threat-awareness information to key stakeholders within the National Industrial Security Program (NISP). The DSS Alexandria 1 Field Office hosted the 2nd Annual Cybersecurity Symposium, which drew more than 82 representatives from cleared industry to the event at the MITRE Corporation facility in McLean, Va.

Significantly, not all industry members at the symposium were facility security officers (FSOs). As DSS transitions to its new methodology focusing on a threat-driven approach, the Alexandria 1 Field Office developed this symposium as an avenue for communicating important cybersecurity information to all necessary partners in the NISP. Thus, the symposium invitations were also sent to information technology professionals at cleared facilities.

Field office personnel, led by Field Office Chief Lisa Savoy, developed the symposium to promote cybersecurity awareness, provide industry with access to field experts from a variety of federal organizations, and encourage private-sector personnel beyond FSOs to engage in building proactive security programs that focus on countering the threat.

Savoy kicked off the event by emphasizing the importance of cross-departmental collaboration to thwart the cybersecurity threat and help protect critical technologies. To further promote threat awareness, CI Special Agent Zach Daniels supported Savoy throughout the day's activities.

To arrange the symposium, the field office coordinated with a number of key government stakeholders, to include the military services and investigative agencies. This coordination resulted in a slate of five briefings presented by the DSS Cybersecurity Division, the U.S. Army, U.S. Navy and the FBI. After solidifying the schedule, the field office sent invitations to all cleared facilities within its area of responsibility. The goal for future iterations of the symposium will be to include more facilities within the Capital Region.

Capital Region Director Justin Walsh closed the symposium by speaking to the industry attendees about the new DSS methodology and critical technology protection, as well as the future of DSS.

Several members of the Alexandria 1 Field Office provided significant contributions to plan and develop the symposium, including Industrial Security Specialists Quantoinette Abney and Steven Saulnier, and participants in the DSS Paid Student Internship Program, Amanda Clary and Nicole Decker, who provided logistical support.

*(**Editor's note:** Lisa Savoy also contributed to this article.)*

Wounded warrior internship provides productive role, promising future

Editor's Note: *The following reflects the thoughts and opinions of the author on his personal experiences as a Wounded Warrior Program intern at DSS.*

by Kenneth Ewen
Tacoma Resident Office

From the first day of military service, someone above me decided my activities for the day. Training activities, physical fitness, field exercises, operations and yes, motor pool Monday all dictated my day-to-day life. The point is, I could predict what tomorrow would look like based on a schedule. I knew what time to get up in the morning, when I would shower, when I would eat and most of the time, when I would head home for the day. I complained about the activities which filled the in-between time just like everyone else: I often questioned why we had to do some activity or extra duty, and how it fit into our mission.

My days grew even longer during deployment. My counterintelligence (CI) team covered an entire base with only a handful of CI agents. This often meant working 14-hour days, and soon the days ran together. I always had something to do. I was always busy. I reported on my activities and jumped to the next thing. I had my routine down, as I always knew what I was doing next. I trained, advised, and assisted until the symptoms of an injury surfaced.

My injuries meant I could no longer remain in a deployed environment. A medical team determined it necessary to remove me from Afghanistan and send me back to the states for medical evaluation and treatment. I didn't want to leave my team and leave them even more understaffed, but what I wanted was not a consideration. I could no longer perform the basic duties of a Soldier. In September 2016, I was medically evacuated from Afghanistan to Joint Base Lewis-McChord, where I would begin the process of transitioning from active duty military service. To say I was angry would be a major understatement.

I was angry because I was injured. I was angry because I left my team to cover for me. I was angry because this new place, the Warrior Transition Unit (WTU), had only one initial purpose for me: medical care and treatment. The very extra duties and tasks I complained about before were gone and, surprisingly, I missed them. I was angry because these medical professionals told me my military career was over. I took this as meaning that my career in the intelligence field was over too. Unfortunately, to my own shame, some of that anger spilled out on the people who tried to help me.

During the preliminary stages of my medical evaluation onboarding process, I was presented with an opportunity for a CI special agent (CISA) internship position with DSS. I jumped at the opportunity. The WTU Operation Warfighter program and the Wounded Warrior Program through DSS provided the possibility for me work a normal job and be productive.

One other service member from the WTU applied for the same position so I had competition. We submitted resumes and had telephonic interviews. I started my internship in April 2017, and my supervisor Ray DuVall, Tacoma Resident Office, treated the internship position as a real job from the very beginning. I submitted Special Access Requests for computer access and had to wait for approval just like a real job. Ray has not pulled too many punches in tasking or training, and has treated me professionally like any other employee he would supervise.

Medically, it has been an interesting year and a half. I have seen specialists outside the military medical system to include doctors at the University of Washington and Swedish Medical centers. I endured several medical procedures, tests and evaluations, and I received support the entire time and genuinely felt the care and concern of everyone I worked with. My medical treatment always took priority, with never a thought of "you're slacking." In fact, Ray has been more cognizant of my medical procedures and recovery than I have.

Professionally, Ray has pushed me to expand my skillsets. I learned a new view of CI and how to communicate CI concerns to civilian companies. I completed training to help my marketability when the military retires me and I learned a lot more regarding analysis of intelligence material. Instead of a two-

year gap in my resume, I filled it with productive and meaningful activities which bolsters my resume and experience base.

I am very grateful to DSS in providing this internship opportunity. I am thankful for the learning opportunities and experience I gained. I did not spend two non-productive years in the WTU with only the concern for my medical treatment. I had the opportunity to help people, learn more about my craft, and have a positive impact on DSS operations in Tacoma all while placing my medical treatment first. More important, by working with DSS, I learned my career in the intelligence field is not over as I initially thought.

As I attend the medical evaluations necessary to determine my fitness for duty which will result in medical retirement, I know my time in the military and my internship with DSS will soon come to an end. However, my future looks good and I have a plan, which is to be a facility security officer where I will apply what I have learned in counterintelligence with yet another viewpoint. I will relocate to Georgia and spend a lot of time with family. I will use my experience, training, and insight to help protect national security interests while working for cleared contractors in Georgia. So, DSS has not seen the last of me.

Kevin Flowers (left), San Francisco Field Office chief, presents a certificate of appreciation to Kenneth Ewen, Wounded Warrior Program intern, at his farewell event. *(Courtesy photo)*

'A Day in the Life'
CDSE holds inaugural shadow day

By Hollie Rawl
Vetting Risk Operations Center

The Center for Development of Security Excellence (CDSE) welcomed 15 students and three career center specialists from Bowie State University and Morgan State University for its inaugural CDSE Shadow Day held November 1, 2018. This immersive experience provided an opportunity for undergraduates to learn about DSS' national security mission and the criticality of training, educating, and certifying security professionals at CDSE to not only protect our warfighters, but to protect the technologies, way of life, and freedoms these students enjoy.

Led by a team of CDSE volunteers, the program began with a command brief on CDSE's missions and supporting elements followed by eight sessions diving deeper into core functions and career specialties. Topics ranged from educational technology to insider threat.

TOP: Security Specialist Instructor Andy Reyes listens intently to Morgan State student Aderoju Awodipe discuss his career goals. **BOTTOM:** CDSE Director Kevin Jones inspires the next generation of leaders during his keynote address. *(Photographs by Marc Pulliam, CDSE)*

During a keynote address, CDSE Director Kevin Jones shared his personal leadership journey, challenging the students to always step out of their comfort zones, look for opportunities in unexpected places, and to never take 'no' for an answer. Jones also divulged CDSE's key to success as the premier leader of security education, training, and professionalization for the DoD and National Industrial Security Program: hiring employees from a wide variety of educational and occupational backgrounds to create one of the most knowledgeable, engaging, and unique cultures within the government workforce.

To provide the students with a classic government experience, Leila De'Vore, Human Capital Management Office, led a Lunch 'n' Learn session focused on key aspects of interviewing, internships, and preparation for hiring and employment.

After lunch, CDSE Shadow Day culminated with employee and student partnerships in a traditional shadow setting. This rare glimpse into the "day in the life" of a security professional included personal conversations about how the student's skills, abilities, and interests pair with rewarding career paths throughout DSS. Goal setting and resume review were also key components of this afternoon collaboration.

Student and employee feedback was overwhelmingly positive, supporting the continuation of Shadow Day into future outreach and recruitments agendas.

Bowie State undergrad Andrea Mwando poses a question to Leila De'vore during the Shadow Day Lunch 'n' Learn session.

New ISR supports local community, agency

by Crystal Diehl
Phoenix Field Office

Alexander Merriam joined the Phoenix Field Office in November 2017 as an entry level industrial security representative. He quickly embraced DSS in Transition and sought out the benefits of the risk-based approach, while completing his National Industrial Security Program Oversight Course.

As an instrumental member of the team, Merriam was heading to Tucson for a follow on meeting on a facility's comprehensive security review. While stopped on the side of the interstate, he heard a loud bang and in his rear view mirror, saw a truck roll from the opposite side of the freeway through the center median into oncoming southbound traffic. Without hesitation, Merriam and another bystander secured the crash site, routing traffic away from the accident and contacted emergency authorities. While awaiting for emergency services, both Merriam and the bystander checked on the people involved in the accident, and then safely pulled them from the ruined vehicle. Upon arrival, employees of the Arizona Department of Public Safety were very appreciative of both parties' efforts related to the accident, and their ability to prevent future harm by rerouting traffic.

As an active member of the Phoenix community, Merriam is involved in the Big Brothers and Big Sisters program, and currently is a sponsor and a big brother of a local student. He coordinated the local Feds Feed Families campaign, is a new member of the DSS Diversity and Inclusion Council, and acted as the area Combined Federal Campaign coordinator. The Phoenix Field Office is extremely fortunate to have him as a member of our team and we look forward to seeing his future efforts in the agency as a new and thriving leader who truly honors community service.

FY18 | DSS by the Numbers

Each year it's a tradition to look back and get a sense of what has been accomplished. DSS is no different. The following are the by the number accomplishments of the agency in FY18:

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

163 **Education Course Completions**

69,299 **Personnel** registered for **webinars**

116,007 **PDUs** [Professional Development Units] **Earned**

88,960 **Visits** to **Security Shorts**

590,554 **Visits** to **Toolkits**

1,401,993 **Course Completions**

1,281 **Conferrals** in Security Professional Education Development Certification Program

NISP AUTHORIZATION OFFICE

28 **NISP Command Cyber Readiness Inspections** led by DSS

5,110 System security plans **(SSPs) accepted and reviewed**

Common deficiencies in SSPs:

1. Management Controls - SSP is incomplete or missing attachments
2. Insufficient justification and description of security controls in place
3. Incomplete risk assessment report

3,923 Completed **system validation visits**

Common vulnerabilities found during system validations:

1. Management Controls - SSP does not reflect how the system is configured
2. Technical Controls - Inadequate Automated Audit Events
3. Management Controls - Unsatisfactory implementation of Plan of Action and Milestones (POA&M)

DOD INSIDER THREAT MANAGEMENT AND ANALYSIS CENTER

571 **Total reports** to the DITMAC

458 **Threshold reports**

113 **Requests** for **information**

31 of 43 **DoD components** reporting to the DITMAC

20 **Components** adopted the **DITMAC system of systems** as their case management tool

103 **Reports** from components based on CE alerts

3 **Non-DoD federal departments** or agencies reporting to DITMAC

CONTINUOUS EVALUATION (CE):

1,120,853 **Subjects** enrolled in CE

390,820 **Army**

291,590 **Industry**

237,059 **Air Force**

129,247 **Navy**

43,913 **Marine Corps**

28,224 **Fourth Estate**

47,453 **Alerts Processed**

3,750 **Risk favorably mitigated**

453 **Risk quarantined** (admin withdraw)

1,132 **Risk transferred** (separation)

116 **Eligibilities revoked**

FOREIGN OWNERSHIP, CONTROL OR INFLUENCE (FOCI)

511 **FOCI** facilities

280 **Mitigation** action plans in place

Analysis

1,546 **Foundational** analysis assessments

321 **Advanced** analytic assessments

Mitigation

61 **New FOCI action plans** (agreements and instruments) negotiated

262 **Tailored FOCI supplements** (AOP/ECP/FLP) negotiated

24 **CFIUS** case responses

Engagements

121 **Annual/initial/renewal meetings**

INDUSTRIAL SECURITY FIELD OPERATIONS

2,379 **Security Reviews** conducted

3,028 **Security Vulnerabilities** identified

2,759 **Non Acute/Critical Vulnerabilities** identified

269 **Acute/Critical Vulnerabilities** identified

1,142 **Facility Security Clearances** issued

25,000 **Substantive CI** & security engagements

1,149 **Substantive violations** processed

INTERNATIONAL ACTIONS

6,153 **Requests** for **Visits**

18,459 **Travelers**/Visitors

317 **Transportation** plans

135 **Hand Carry** plans

1,688 **Clearance assurances**

COUNTERINTELLIGENCE

49,678 **Reports of suspicious contact** from industry

5,394 **Referrals to Law Enforcement**/Intelligence Community

372 **Investigations/operations opened** due to DSS referrals

3,229 **Intelligence Information Reports**

4,344 **Personnel** attending three **secure VTCs** with industry

VETTING RISK OPERATIONS CENTER (VROC)

839,000 **National Industrial Security Program (NISP) contractors** with **clearance eligibility**

740,000 **NISP contractors** with access to **classified information**

168,168 **Requests** for **investigation** for **security clearances processed**

84,328 **Interim security clearance** determinations made

9,588 **Adverse information** reports triaged

181 **Interim suspensions processed** (actual suspensions, not LOJs)


MANAGEME