DSS ACCESS

Official Magazine of the Defense Security Service | **Volume 6, Issue 4**

THIS ISSUE

Mobile course helps identify, counter cyber threat

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

Chief of Staff | Troy Littles

Chief, Public Affairs | Cindy McGovern

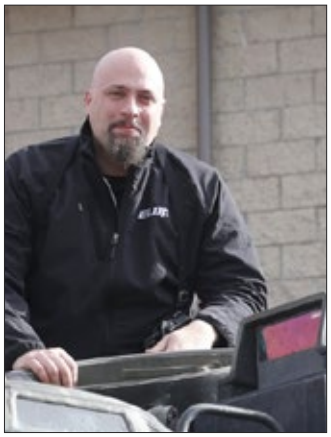
Editor | Elizabeth Alber

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: MOBILE COURSE HELPS IDENTIFY, COUNTER CYBER THREAT

INSIDE

AROUND THE REGIONS

ASK THE LEADERSHIP

From the Director

As we close out 2017, it's a tradition to look back at the previous year's accomplishments and assess our goals for the new year. DSS established five overarching goals for 2017 and I want to briefly touch on each one:

- Workforce Development
- Risk-based Approach (DSS in Transition)
- DoD Insider Threat Management and Analysis Center (DITMAC)
- Defense Security Enterprise Transformation
- Information Technology and Cybersecurity

DSS has made leadership development a priority and stood up a formal program open to all employees based on a two-tier approach that concentrates on specific grades. Tier I includes GG7 – GG13 employees and Tier II includes GG14 – 15 employees. This 12-month program includes formal in-classroom training, self-assessments, coaching and reading assignments. By the next issue, we will have completed our first round of workshops and hear feedback directly from the participants.

DSS in Transition remains a dynamic, fluid model that has dramatically evolved in the past year. After the new approach was designed, we formed integrated process teams (IPTs) to develop each component of the new methodology into an efficient, effective, and repeatable process applicable to all cleared facilities. The IPTs completed draft concepts of operation (CONOPS) for each component of the new methodology. In August we updated, refined, and integrated the individual component CONOPS into a single, unified, and aligned process.

We then launched two planned practical exercises to operationally test the integrated CONOPS. The first is scheduled to run through February 2018; the second started in November and ends in March 2018. The second exercise will incorporate the early lessons learned and best practices from the first practical exercise. The next step, in early 2018, will be a pilot of the integrated CONOPS that will involve all four DSS regions and will focus on facilities of varying complexity. The goal of this pilot is to ensure the new methodology is scalable and applicable to all facilities in the National Industrial Security Program. I firmly believe that "Partnering with Industry" is key to the success of this initiative and look forward to sharing the results from this exercise with you.

DITMAC achieved initial operating capability late last year and continues to serve as the enterprise-level capability for insider threat information management. And in March, DITMAC was directed to establish an Insider Threat Enterprise Program Management Office. We continue to mature DITMAC as we explore additional data systems, as well as behavioral science to define our products and develop a holistic picture of potential insider threats.

We accomplished a number of milestones in transforming the Defense Security Enterprise. We continue to enable a tighter integration between counterintelligence and security, not just in DSS, but across DoD and industry. We developed and are prepared to fully execute new missions such as Continuous Evaluation, Unauthorized Disclosure and industry insider threat program requirements. And, we continue to identify and counter foreign intelligence cyber activities through our support to national cyber initiatives and collaboration with key stakeholders and partners.

Finally, we are on the cusp of delivering technological solutions and a robust data environment to the industrial security community. Soon, we will deliver the National Industrial Security System which will replace antiquated systems and become the system of record for facility clearance information.

It's been an extremely busy and productive 2017 for DSS. I look forward to the challenges of 2018.

Dan Payne
Director

Course focuses on CYBER THREAT, incorporates mobile travel team format

by Beth Alber
Office of Public and Legislative Affairs

The cyber threat from foreign intelligence and criminal actors has risen and is affecting many aspects of the DSS mission to protect classified information and technologies in cleared industry.

Recognizing the enormity of the threat, the DSS Counterintelligence (CI) Cyber division realized that the CI and the industrial security work force needed an integrated approach to identify and counter this threat, noting that the threat had significant differences from human intelligence in methods and capabilities. The team concluded that it should develop an interactive training curriculum for the work force, and sought a partnership with the Joint CI Training Activity (JCITA).

Initially, the audience was CI special agents and CI analysts; but eventually industrial security representatives and information systems security professionals (ISSP) also attended, creating an opportunity for a more collaborative and ready force to work with cleared industry against the cyber threat.

The course concept was developed by Donald Reese, Todd Tucker, Mike Berry and Mike Monroe of CI Cyber. After a year of coordination with JCITA, what evolved was "The Cyber Threat Intelligence Seminar," a three-day mobile travel team format that was conducted in each of the DSS regions during the past year.

"In the complex environment that cyber presents; building specific training to assist DSS field personnel was an imperative," said Todd Tucker, chief, Cyber Operations for the division. "Our aim was to build the understanding of

cyberspace from the CI perspective as it affects cleared industry."

The training is comprised of several blocks of instruction, with the first day focusing on the basics of cyber with an overview of cyber terms and definitions, a discussion of network functionality and design, followed by further instruction on network information security.

"This was an eye opening experience," said William Gawler, ISSP in the Alexandria Field office. "The seminar provided a different perspective that we don't always get to see as ISSPs, and the information will be very valuable out in the field."

"You will get a Cyber 101 course on the first day, which will teach you the basics of how a router and the internet work," said Mitch Wells, CISA in the San Diego Field office. "For those that are more advanced, it will seem very elementary, but at the end of the course, beginner and advanced students will have taken something away from the course."

On the second day, students review a plethora of current cyber tools to cull data from open sources in support of their mission, focusing on identifying a scam versus a valid contact; the tools used by foreign intelligence entities targeting networks; and a complete threat picture of each country's cyber actors and their typical mode of operation.

On the third day, the instructors go through specific DSS suspicious contact reports to identify good reporting and what's not so good. "The instructors break down each example with the class after providing them an in depth list of follow up questions typically used after a cyber event," said Tucker, "with the goal of getting the best reporting out of cleared industry."

A discussion also focuses on coordination with other government agencies, which is critical to identifying trends in cyber activities and issues. The discussion outlines specifics on agencies' investigative and operational interests, as well as pointers on what other government agencies that are the powerhouses in the cyber environment and how best to utilize them.

"This is a class that I believe all ISSPs need to attend," said Alex Stead, ISSP in the Chantilly Field office. "This is hands down one of the best classes I have attended."

"The course proved effective in outlining the major cyber threats and in providing some level of familiarity regarding indicators, defense and significant reporting expectations," said Michael Pilla, industrial security specialist in the Philadelphia Field office.

"This particular training course gives the student tools they can actually use in the field," said Wells. "There are several recommendations and tips given by the instructors that I took away and I am currently using now."

After going through the Cyber Threat Intelligence Seminar, the students will know the key aspects of the current threat environment and have the knowledge to develop a repeatable process to improve the dependability, quantity, quality, and agility of reporting on a cyber-attack. "The feedback received from the attendees was very positive," said Tucker, "with an overwhelming desire to have this seminar continue in the future."

The plan is for the training to transition to support CI personnel from all services at JCITA in fiscal year 2018. DSS will then work with JCITA to schedule more mobile sessions at DSS locations, and qualify DSS personnel to attend the in-residence version.

Acquisitions overcomes deficiencies to achieve successful procurement management review

by Tara Petersen
Chief, Office of Acquisitions

Editor's Note: The author joined DSS in March 2016, right after the final PMR report arrived. Before joining DSS, she was the PMR program manager at the Defense Contract Management Agency (DCMA) who led the 2015 review of DSS, providing her a good idea where to begin preparations for the PMR re-assessment.

The DSS Office of Acquisitions (AQ) successfully accomplished its number one goal for fiscal year 2017 -- achieving an outstanding result from the supplemental Procurement Management Review (PMR).

DSS underwent an initial PMR in June 2015 that found systemic documentation deficiencies in a sample of files reviewed, indicating potential widespread non-compliance with regulations and process requirements. The PMR team's out brief reflected high concern that DSS contract arrangements may have led to poor business deals, wasted funds, or unenforceable contracts, and DSS was on the verge of losing procurement authority. The PMR team identified 34 recommendations to correct regulatory findings and the Office of Defense Pricing/ Defense Procurement and Acquisition Policy (DPAP) directed an early re-assessment.

Some Background

The DoD provides oversight of delegated procurement authority through the PMR Program executed by the DCMA on behalf of the director, DPAP, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. The purpose of the PMR program is to ensure agencies are exercising procurement authority in accordance with rules, regulations, policy and best practice. DCMA inspects the contracting activities of 21 Other Defense Agencies and Defense Field Activities on a rotational basis so each office gets a review once every three to four years.

The Immediate Response

AQ didn't wait for the final PMR report to begin corrective action; in fact, even before the PMR team left, internal review thresholds were lowered to provide greater oversight of contract execution and to ensure compliance of contracts. Internal training was also immediately conducted to address knowledge gaps identified in the PMR outbrief. The final PMR report was received in March 2016, and the PMR team was scheduled to return in June 2017.

Changes were needed across the spectrum of operations and numerous initiatives were undertaken to update processes and internal policies, and introduce accountability for compliance. Key improvement efforts focused in three main areas -- provide more time for proper processing of contracts, improve knowledge of all players in the process, and ensure the documentation clearly shows compliance.

Time

The PMR report noted a prevalence of compressed and unrealistic timelines given to AQ by DSS customers for processing contracts, a contributing factor to the lack of documentation and non-compliance. Customer expectations for speed of execution did not align with regulatory process requirements. To address this issue, AQ published a new Procurement Administrative Lead Time (PALT) table to provide adequate time for acquisitions and serve as a tool to support planning for timely submission of purchase requests. This table also helped to re-frame customer expectations. Adherence to published PALT was tracked, which enabled analysis and accountability. Fiscal year-end submission deadlines were also published early to enable customer planning, and support of DSS leadership led to more timely submissions. These efforts provided AQ the time needed to meet regulatory requirements and still support customer mission needs.

Knowledge

Knowledge was addressed on multiple fronts; technical knowledge of the AQ staff, educating customers with respect to their role in the process, and keeping leadership informed. Training and dialogue among the AQ staff promoted consistency in application of guidance and execution of requirements. More frequent interaction and coordination with support elements and customers improved understanding of purchase request package requirements and the intricacies of

a complex acquisition process. This also led to more realistic expectations. The draft PMR report provided to AQ for comment stated, "AQ has made outstanding progress communicating, training and coordinating with their customers to promote mutual understanding of their procurement process responsibilities." Establishment of metrics improved knowledge of the health of contract operations. By tracking workload execution and file review results, trends were identified and root causes pinpointed, guiding process changes. Metrics also enabled communication to directorates and DSS leadership. Improved understanding of all stakeholders drove improvement in the contracts.

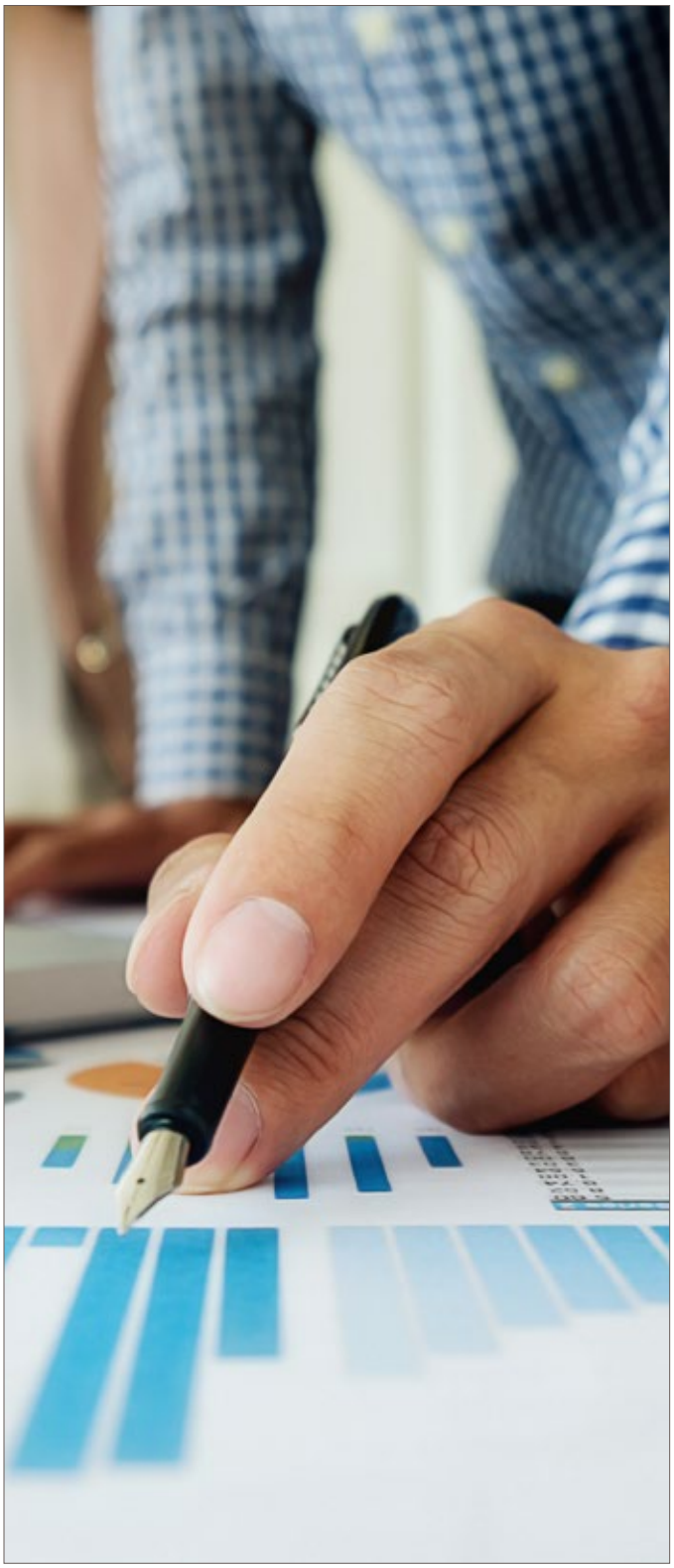
Documentation

Finally, the documentation had to demonstrate compliance. Review of contract files is the primary means a PMR team has to determine if contracting processes are executed appropriately. Documentation deficiencies were addressed through training and a robust oversight program consisting of in-process file reviews and a post-award self-inspection program. Results of these reviews were tracked and analyzed and trends informed training to achieve improvement in future documentation.

PMR Results

The PMR team commended DSS for "significant improvement in the procurement process, contract administration and personnel performance in the acquisition organization." The draft report stated "the more recent contract files the PMR Team reviewed were outstanding in comparison to contract actions prior to fiscal year 2016. In regard to following established internal policies, operational instructions and compliance with regulations the contract files are demonstrative of significant improvements in AQ." The report also stated "communication between the Acquisition Office and their customers throughout the agency has become more integrated with all parties involved in the procurement process as early as possible. Leadership in the agency and the Acquisition Office has transformed the morale and professionalism of the work force." The PMR team only identified two recommendations to address regulatory findings as a result of the 2017 review, representing a drastic reduction from the 2015 PMR. Not only was DSS procurement authority preserved, John Klar, the PMR team lead, stated, "DSS has made some remarkable improvements in the Office of Acquisitions."

When asked what she felt was the one thing that enabled AQ's success, Ashley Maddox, Contract Operations branch chief stated, "The team that we have has played the biggest role in our success -- from the AQ leadership to the contracting officers and contract specialists working here. They are all so dedicated to the mission and supporting this office and their customers successfully. Without each of them, we would not have been successful in making any changes to this office."



A Q&A with **Tara Petersen**, Chief, Acquisitions Office

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

Tara Petersen joined the DSS team in March 2016 as the chief of the Office of Acquisitions (AQ). This office is responsible for purchasing the goods and services that support DSS and its mission. AQ exercises delegated contracting authority through award and administration of contracts, providing required approvals for interagency acquisitions and inter-service support, and serving as the acquisition/business advisors to all directorates within DSS.

Prior to her assignment to DSS, Petersen served as the director of the Procurement Division at the Defense Contract Management Agency (DCMA), where she directed all procurement activities providing contract support to DCMA. She also managed the Procurement Management Review (PMR) Program on behalf of the director, Defense Procurement and Acquisition Policy to assess the overall health of contracting operations at 21 Other Defense Agencies and Defense Field Activities.

Petersen entered federal service in November 1994 under the Air Force's Copper Cap Internship Program, F.E. Warren AFB, Wyo. She graduated in 1996 and earned her first contracting officer's warrant shortly thereafter. During her 23 years of service, she has held a variety of positions with increasing responsibility spanning all aspects of operational contracting. Her leadership experience includes director of business operations positions for the 10th Contracting Division, U.S. Air Force Academy, and the 700th Contracting Squadron, Kaiserslautern, Germany. She then became the deputy chief of the, Contracting Division, Directorate of Logistics, Installations and Mission Support, Headquarters U.S. Air Forces Europe and Africa, before taking the job at DCMA.

She graduated from Utah State University with a bachelor of science degree in liberal arts and sciences. She has received numerous quarterly, annual, and performance awards, the Air Force Space Command Outstanding Contracting Civilian of the Year Award, and two Meritorious Civilian Service Medals during her career.

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

During my 23 years, I moved around a lot to gain new experiences, and to build depth and breadth in my knowledge of acquisition operations. I worked my way up from a contract specialist to leadership positions at the squadron level and on headquarters staff as the deputy chief of Contracting for the United States Air Forces in Europe. After spending five plus years in Germany, I took a job with the DCMA that included management of the DoD PMR Program. I was responsible for the review and assessment of the contracting operations at other Defense Agencies and Defense Field Activities. I was introduced to DSS through that position. I led the team that conducted the PMR at DSS in 2015, which had identified systemic deficiencies and non-compliance in the contracts reviewed. When the DSS chief of acquisitions position became available, I was intrigued by the challenges indicated by the PMR and pursued the opportunity. I then found myself in a unique position of having been responsible for writing up the organization I was now charged with leading, and having the responsibility to fix it.

Q: What are the biggest challenges for the acquisition office at DSS?

I think the biggest challenge we face here is ensuring adequate time to execute contracts in a dynamic and changing environment. The contracting function is governed by numerous laws, regulations and policies, which dictate our processes. Every requirement brings with it a unique set of circumstances that we must analyze to determine applicability of the guidance and which processes to follow. We also must fully understand what

it is we're being asked to buy and we need to determine if there are sources that can meet those requirements, so research must be conducted to determine an acquisition strategy. All of this takes time to work through and often our customers can't give us the time we need, so the acquisitions staff is challenged to be creative, agile and responsive to meet the rapid pace of change here at DSS.

Q: What was your focus when you initially took the position?

My primary goal on arrival at DSS was to get the office ready for the return PMR driven by the 2015 review, and of course, that had to be done while continuing to meet the contracting needs of the agency, as well as successfully closing out the fiscal year. It was like having to fix multiple cracks in an airplane mid-flight, ensuring the plane landed safely, and then getting the inspector to say "what a great plane you have there." The issues identified in the PMR pulled our focus in various directions since the findings addressed problems across the spectrum of operations, but achieving an outstanding result on the next review was the goal we set and kept in our sights.

Q: The Acquisitions Office recently had a vastly improved PMR. What can you tell us about that? How did the office effect change? What still needs to be done?

A substantial number of changes had to take place to correct the trajectory of the office and retain procurement authority for DSS. I think the success we achieved derived from two fundamental things we put into place very early: tracking mechanisms and robust oversight. The data is the key. If you don't know what's going on, how do you know what changes to make? Our analysis of the data drove the changes. We started with the PMR report, then the data we gathered from various metrics, pre-award contract reviews, and a post-award self-inspection program, which informed all decisions and provided feedback on whether our initiatives were in fact achieving what we intended. When the data showed us we weren't hitting the mark, we adjusted. When the data confirmed the improvements we were looking for, we celebrated and built on that success. We also continually refined our metrics to gain further insight into our operations and the impact of the changes we made. My staff was another critical component. They were hard working, mission focused, and dedicated to getting our operation to where it needed to be. They embraced the vision and the goal, and did the work. We continue to make improvements based on regular analysis of the data, and seek out efficiencies so that we can provide more efficient and effective contract support. This process is our new normal.

Q: Can you explain the role of the COR? Who do they assist in the Acquisitions Office?

The COR is the contracting officer's representative. CORs are delegated specific responsibilities by the contracting officer and are critical to ensuring DSS receives the services required in a contract. CORs are the technical or subject matter experts who have the most in-depth knowledge of contract requirements. The contracting officer relies on the COR to be their eyes and ears as they provide surveillance of contracted services and accept those services on behalf of the government. If problems or issues arise, the COR works with the contracting officer to enforce contract requirements and work through those issues to get the contractor back on track.

Q: What future goals do you have for the Acquisitions Office, and how do you plan to achieve those goals?

Goals at the top of my list right now include:

- Enable DSS in Transition, and if DSS is directed to take the background investigations mission, provide flexible and adaptive contracts to meet changing requirements
- Create a pipeline into DSS Acquisitions with establishment of an intern program
- Create a work environment that draws talent. This entails providing learning opportunities and empowering the workforce to make a difference.
- Provide effective training resources that help customers understand the complicated acquisition process and navigate requirements for submission of purchase request packages
- Continually improve communication between acquisitions and all stakeholders to enhance support provided

We'll approach these goals the same way we approached preparation for the PMR. We'll brainstorm ideas on how best to achieve each goal and create plans of action. Then we'll assign responsibility and implement tracking mechanisms to monitor progress. We'll seek feedback and adjust as necessary, then we'll build on successful achievement.

Training paves way for full RMF Implementation

by Selena Hutchinson
Industrial Security Field Operations

DSS began a phased transition to the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) in October 2016 and full implementation is set for Jan. 1, 2018. The NIST RMF is a common security framework designed to help federal organizations improve information security and strengthen risk management processes. RMF is a multi-tiered approach that provides a disciplined and structured methodology for integrating federal security related standards and guidelines into a comprehensive enterprise-wide security program.

Information systems security professionals (ISSP) oversee the implementation of RMF in industry and received the latest guidance during training held in August at the Center for Development of Security Excellence in, Linthicum, Md. Attendees benefited from technical presentations provided by their peers and nationally recognized corporate information security leaders.

For the past two years the National Industrial Security Program Authorization Office (NAO) has taken on the task of addressing and training to the challenges of implementing the framework. RMF is a shift for all cybersecurity professionals nationwide to transition away from the schedule-driven checklist mentality of certification and accreditation, and to embrace the

Tiffany Snyder, an information systems security professional from the Melbourne Field Office, briefs on assessing security controls.

changes and more than 380 security controls inherent with RMF implementation. It is imperative that ISSPs centrally train to understand the challenge DSS faces making these wholesale changes, both internally and with industry and other government partners.

A couple of new elements were added to the training this year to improve efficiency and consistency, such as minimizing the use of PowerPoint and using ISSP trainers.

"ISSPs are smart and incredibly adaptable not just because of their skills but because of their attitudes. They are the leaders of RMF," said Karl Hellmann, NISP Authorization Official. "The transition will only succeed if they buy in and echo the need for consistent implementation of this complex guidance."

That's why Hellmann insisted that several ISSPs provide technical presentations during the training. The volunteer presenters were: John Forster, Pittsburgh Resident Office; Renee Lumpkin, Atlanta Field Office; Luis Morales, Hanover 1 Field Office; Victor Natividad, Mt. Laurel Field Office; Hung Phan, Andover Field Office; Tiffany Snyder, Melbourne Field Office; and Gary Sims, Irving Field Office.

The hands-on training ensured the latest and most accurate training information, templates, and other artifacts were made available to DSS personnel as the RMF process continues to evolve. It also created synergies across the field, which helps to eliminate inconsistencies, focus on repeatable processes, and ultimately provide consistent results.

The Defense Information Systems Agency provided a two-person team to train on the Enterprise Mission Assurance Support Service (eMASS) application which will be used by both DSS personnel and cleared industry to coincide with full RMF implementation. The eMASS application will replace the ODAA Business Management System, and is a DoD-owned web-based resource that automates the RMF process. It includes all the reports required by the RMF process, and it generates new reports based on the user's needs. The main vision for eMASS is to allow users to share access to specific data in near real-time and in a secure manner.

Lindsay Rambler-Johnson, DRS Corporate information systems security manager and director, Cybersecurity Audit, presented, "Industry RMF Implementation," providing a perspective from the industry side. The SANS Institute provided technical presentations from two leading cybersecurity experts. James Tarala, a

senior instructor with the SANS, briefed the group on "Practical Security via the RMF and the CIS Critical Security Controls." Kelley Dempsey, senior information security specialist at NIST, presented the status of SP 800-53 Revision 5, NISTIR 8170 draft (on a blended approach to managing risk - blended between the RMF and the cybersecurity framework), NIST SP 800-171 Revision 1 (protecting controlled unclassified information in nonfederal systems) and the upcoming 800-171A which will detail assessment procedures for the requirements in 800-171 Rev 1, and also a little bit about NISTIR 8011 on automating assessments.

Attendees received continuing professional education credit by attending the RMF Refresh Training, fulfilling the requirement to maintain DoD 8570 certifications. The ISSPs and other presenters also had opportunities for networking, professional development, and a centralized forum to address inconsistencies.

Annual FOCI conference focuses on mitigating threats, sharing best practices

by Matthew Kitzman & Raphael Turner
Industrial Security Integration and Application

In July 2017, DSS held the 21st annual Foreign Ownership, Control, or Influence (FOCI) Conference for companies operating under FOCI mitigation agreements at the U.S. Patent and Trademark Office in Alexandria, Va., and via videoconference to DSS field offices across the country.

In breaking with previous conferences, this event took place over one day rather than multiple days. It brought together almost 375 outside directors (OD), proxy holders (PH), and facility security officers (FSO); representatives from law firms and consulting firms; and government participants from various Department of Defense (DoD) and non-DoD departments.

In his remarks opening the event, DSS Director Dan Payne set the stage with two main points. First, he said DSS must change as an organization if it hopes to combat the persistent and enduring counterintelligence threat facing the U.S. and the defense industrial base. Payne made clear, "the economics and the success of... companies is just as important to our national security as is any protections that [DSS] would put on the technology itself or the information" held or produced by industry.

Booker Bland, DSS Counterintelligence Operations Analysis Group, describes DSS's role in dealing with insider threats from within industry.

Second, Payne elaborated on the unprecedented counterintelligence threat to the U.S., and specifically how one potent adversary "has truly found the key to use business as a weapon."

The conference was divided into six sessions, including an applied case study on DSS in Transition (DiT), a roundtable presentation on OD/PH standards reform, a panel on Government Security Committee (GSC) best practices and challenges, a briefing on the supply chain threat, a panel on insider threat best practices, and a presentation from an OD on addressing the cyber threat.

During the applied case study on DiT, Gus Greene, director, Industrial Security Field Operations and Andrew Winters, Capital Region action officer, along with FSO Brian Prioletti, summarized the first full-scale test of the new DSS methodology. The presentation focused on the participation between DSS, the cleared contractor, and the government risk owner to identify and prioritize the assets of the facilities, as well as conduct a full analysis of the vulnerabilities to the facilities taking NISPOM compliance and specific threat information into account. The results of the analysis will be used to develop, in partnership with the contractor, a tailored security program that combines NISPOM compliance and threat-informed mitigation measures.

The roundtable on OD/PH standards reform focused on recent engagements between DSS and industry partners with an aim toward creating a more robust approval and oversight process for OD/PHs. The panel members provided their insights into what it means to be an effective OD/PH, and the role DSS should play in the oversight of these positions. Highlights of the panel included the balance of skill sets on the board, the use of internal and external evaluations of board members and boards, and training requirements for OD/PHs. Ultimately, the OD/PHs, and company board as a whole, should be placed in the best position "not just to ensure that bad things don't happen, but actually to be an enabler that good things do happen," one panel member said. Therefore, the company board, in conjunction with DSS, must position themselves in a way as to be capable of filling the vacuum created when a shareholder is told

that there are areas, information, or issues they cannot be involved in with the company.

During the GSC panel on best practices and challenges, industry participants on the panel conveyed that it is the OD/PH's responsibility to fix issues at companies as they arise, inform DSS, and seek assistance or guidance throughout the process. Accordingly, OD/PHs must make training their responsibility, be curious, understand the parent, over communicate, and in the end, take ownership of the FOCI compliance program.

The supply chain threat briefing, provided by William Stephens, director, DSS Counterintelligence, noted that the CI information provided by industry shows the U.S. is losing its battlefield technological advantage. The U.S. must create a unified strategy to secure its supply chains to ensure the delivery of necessary critical technologies uncompromised. Quoting an unnamed foreign intelligence official, Stephens relayed the official's statement that his country could meet their intelligence requirement in Crystal City. Stephens concluded with some questions to use in the OD/PH's oversight roles, including whether company CI and security staff understand the value the company adds to technology and whether the company is aware where the risk is in their supply chain.

The insider threat best practices panel discussed the importance of mature insider threat programs for both security and business concerns, noting that a quality insider threat program will allow a company to increase its competitive advantage in the marketplace and discover those issues that are outside normal operations. According to industry participants, companies are going to do what is necessary in this area to protect its technology and information.

"It is the job of an OD/PH to ensure the protection of a company's unclassified cyber networks, and in many cases this is something that today's boards are not specifically trained to address," said Outside Director Robert Reynolds during a session on addressing the cyber threat. However, industry must gain some perspective on the issue, noted Reynolds, and that adversaries, generally, are conducting cyber operations on a budget and using methods such as phishing, weak passwords, vendor network access, and poor cyber security policies. Industry must consider the threat and vulnerability to their IT systems and the impact to data if it is lost. Once the overall risk is determined the company must make it difficult to penetrate systems, not impossible.

DSS Deputy Director James Kren provided a wrap-up of covered topics and takeaways for the participants. First, DSS armed the participants with additional ideas to perform their security oversight role more effectively. Second, DSS ensured participants heard about and had an appreciation for the different roles involved in a superior security program. Third, DSS worked to increase awareness and understanding of DiT and specifically how it applies to the FOCI community. Fourth, DSS provided a baseline understanding for the stakeholders on several themes, to include the need for government and industry to lead together, to work security into the acquisition process early on, and for strategic engagement between DSS and foreign shareholders.

TOP: The Honorable Dov Zakheim, outside director and former Under Secretary of Defense (Comptroller,) explains the importance of the outside director/proxy holder role in the industry board of directors. Panel moderator Nicoletta Giordani, Industrial Security Integration and Application (ISIA), listens. **BOTTOM:** William Cooper, ISIA, elaborates on the need for cooperation and interaction among members of the corporate Government Security Committee, while panel moderator Allyson Renzella, ISIA, listens. *(Photos by Derik Bland, ISIA)*

Understanding the facility clearance process

by Larry Pyles
Facility Clearance Branch

When following the yellow brick road to a facility clearance, it isn't the great and powerful Oz that you find at the end, but rather the Facility Clearance Branch (FCB).

The FCB processes facility clearances for all four regions and 26 field offices nationwide. When a facility is sponsored for a facility clearance, usually by a government contracting activity, an FCB staff specialist is assigned to the in-process facility and will review the DD Form 254 and sponsorship documents for accuracy and completeness. Once the package has been thoroughly reviewed, it is either accepted or rejected. If accepted, it is then assigned to a security specialist, who schedules a telephone survey with the facility points of contact.

The sponsored facility will receive email notifications at every step of the FCL process to keep information flowing freely and prevent unnecessary delays. In one of the first emails, the facility receives the FCL Orientation Handbook, which will provide a "road map" to the process and explain what items will be important such as the organizational structure and documents of the company (e.g., Incorporation, Limited Liability Company and so on). The handbook and the Facility Security Officer toolkit can also be found on the DSS website in the "most requested links" section. FCB encourages a thorough review of the handbook, as well as the toolkit early in the process (within the first five days) and before the telephone survey to help prompt questions to ensure a clear, complete and mutual understanding of the process, and expectations.

Not every sponsorship package is accepted. On average, FCB rejects approximately 46 percent of all facility clearance requests received. Some of the more common rejection reasons are:

- Missing government contracting activity authorization
- Incomplete sponsorship request-missing critical information
- Incomplete DD Form 254
- Conflicting information on the sponsorship request and the DD Form 254
- No justification for access to classified information

The telephone survey is conducted within the first 10 days of the clearance process, and is the first step in the partnership between DSS and the contractor. Communication is critical in establishing the foundation of this partnership. Being proactive is very important to

the process and will ensure a seamless transition toward the next steps, and it will also be beneficial to mitigating the discontinuation points that could potentially stop the FCL process.

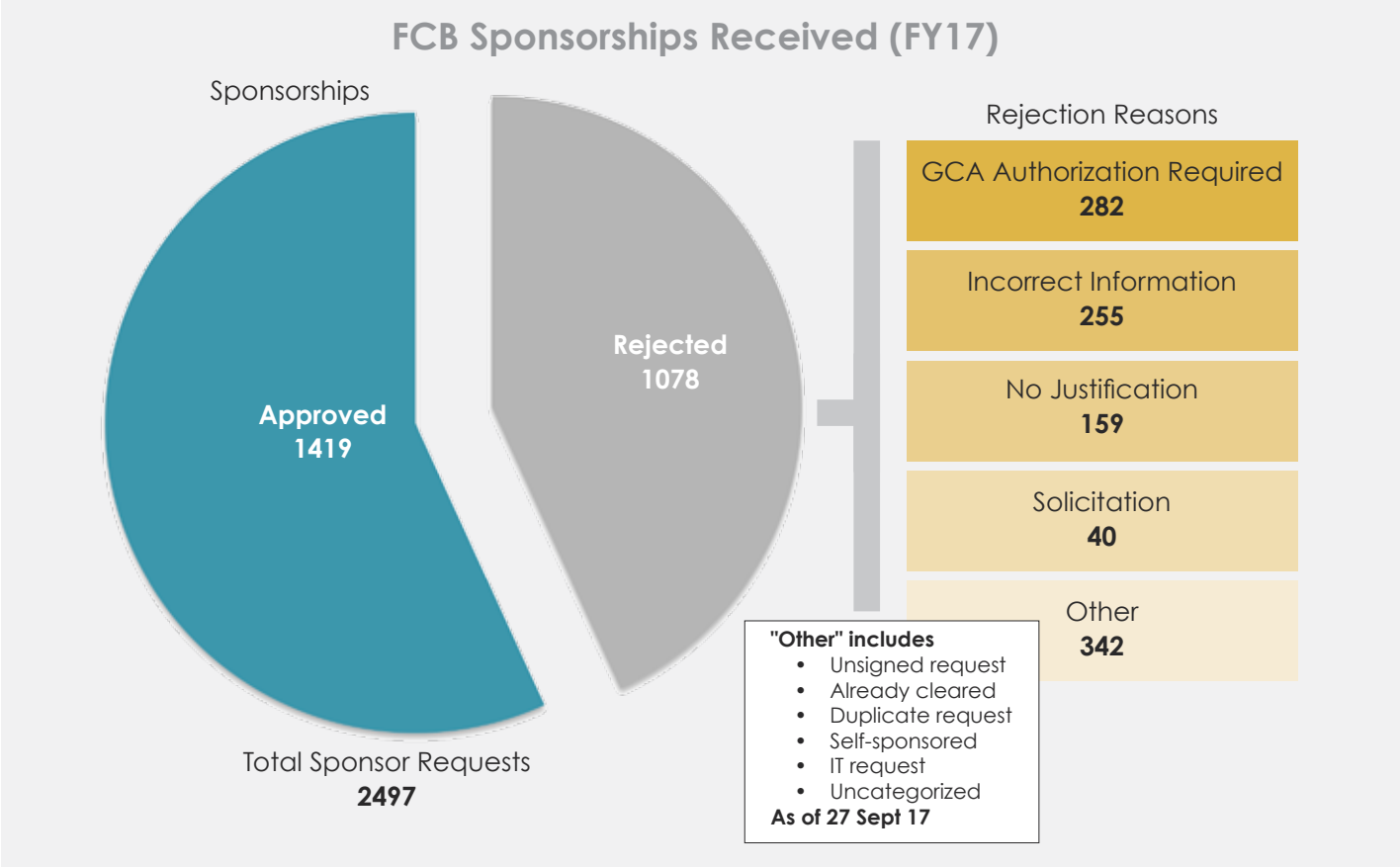
The critical part of the process is the submission of all required business documents, and a complete and thorough package must be submitted by day 20. This discontinuation point is communicated to the facility on the day the FCL Orientation Handbook is sent in the welcome email. This date is also emphasized during the telephone survey and must be met or the FCL process will be discontinued. If the submission is rejected then a sponsorship re-submission will be required and the process starts over.

Accurate information is necessary for the seamless transition through all phases of the process, and the key management personnel (KMP) list is no exception. This requirement is necessary for DSS to initiate personnel security clearances for KMPs in the corporate structure. This information will be requested up front as soon as possible because this is often the most time consuming part of the process. KMPs must access the Electronic Questionnaire for Investigative Processing (eQIP) system within 30 days or before the 45-day discontinuation point, or the FCL process will be discontinued. Electronic fingerprints must also be submitted via Secure Web Fingerprint Transmission within 14 days or the eQIP application will be rejected.

An industrial security representative (ISR) will visit the facility between days 20 and 45 after the e-FCL has been approved and the KMPs have submitted the eQIPs. This visit serves as an introduction to the National Industrial Security Program (NISP) and to the ISR, who reviews all pertinent information and documentation, as well as NISP requirements.

The final step of the facility clearance process is the adjudication of personnel security clearances for the KMPs. Once all the KMPs have been granted personnel clearances, the FCB will issue the final FCL. The keys to successfully navigating the facility clearance process are adhering to the timelines, having accurate and complete information, asking questions, and keeping DSS involved along the way. Just remember to ask questions at every step of the way and keep DSS involved in your security program.

As a note on the systems used to process information, the Electronic Facility Clearance System and the Industrial Security Facilities Database are transitioning to the more efficient, user-friendly National Industrial Security System which will roll out in the near future.



Virtual conference highlights trends, changes, challenges

On July 26, 2017, the Center for Development of Security Excellence (CDSE) hosted its second Virtual DoD Security Conference. The theme for the conference was "Trends, Changes, and Challenges."

As a result of the rising demand for guidance and policy, and practicing best cost saving solutions, DSS was able to leverage new technologies to meet the demand for greater engagement and collaboration for the security community. This year's security conference allowed more than 1,400 security professionals from over 40 different agencies and services across 15 countries to participate. This year saw double the amount of attendees from the previous virtual conference. Rather than travelling to a central location, the collaborative, online platform enabled attendees and speakers to participate from their homes and offices.

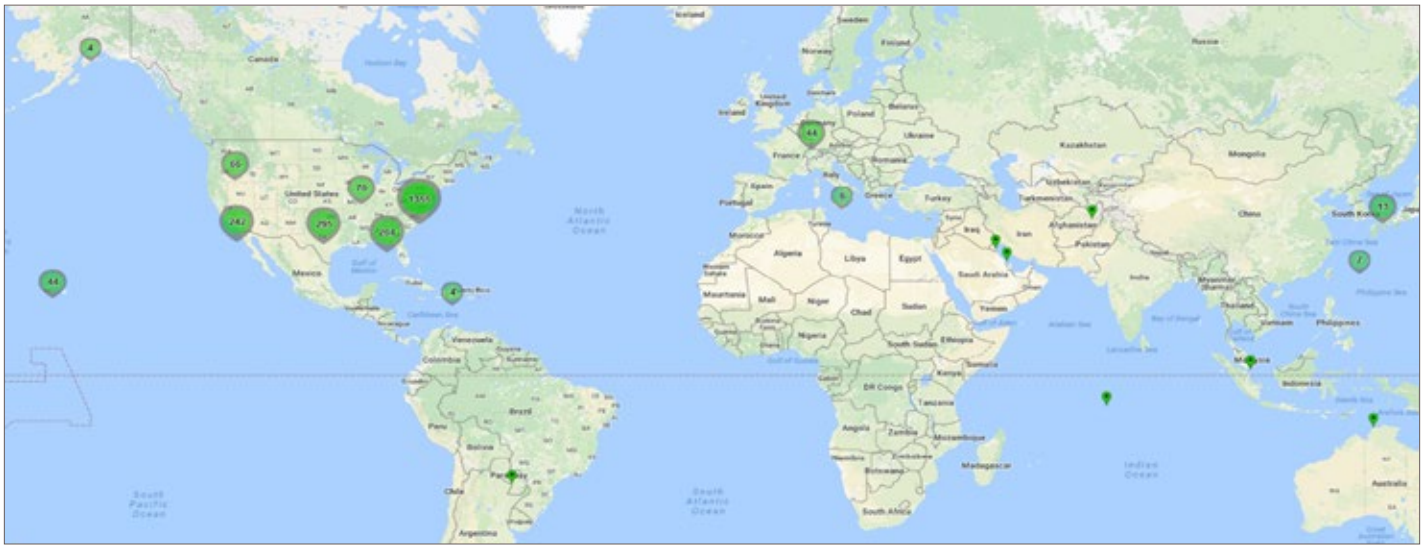
Using the virtual delivery capability, lodging, travel, and administrative costs were avoided. The conference addressed the immediate needs of the DoD security community while bringing civilian and military security professionals together from all over the world.

CDSE worked with the DoD Security Training Council to establish a working group to select session topics that represented the community's needs. Specific conference sessions included:

- New adjudication guideline implementation
- Controlled Unclassified Information (CUI) policy implementation and CUI markings
- New DD Form 254 process
- Changes to information security policy
- Personnel security policy updates, tiered investigations, and the way ahead
- Physical security focused on wireless and personal electronic device impacts

Attendees participated in the conference for an average of 5.7 hours per attendee, dedicating 488,151 meeting minutes covering seven specific DoD security updates.

Participants appreciated the delivery platform and topics, one saying that the conference was "very useful and professional delivery in this annual conference. [The online platform was] a tremendous resource that should continue to be utilized. Would ask for consideration to schedule or deliver additional briefings more frequently than an annual basis."



Worldwide Participation in the 2017 Virtual Security Conference.

Program develops future DoD executive leaders through immersion, academics

The DoD Executive Leadership Development Program (ELDP), offered annually, gives participants a big-picture view of military concepts and routine missions. The program is designed to enhance the experience of military and civilian employees advancing to senior leadership positions within the department. Graduating from the program in June were Amanda McGlone, Facility Clearance Branch, and Dustin Sievers, Virginia Beach Field Office.

Established in 1985, ELPD identifies and develops future DoD executive leaders and improves the quality of civilian DoD employees. The program also provides exposure to senior military officers and civilian executives, introduces new concepts along the development continuum, and offers virtual sessions for continued learning and practical application for an unparalleled and challenging training experience.

Below are the first-hand experiences of the DSS employees.

Amanda McGlone

The ELDP is designed to give participants a better understanding of the DoD enterprise – from talking to an Army private first class at the Demilitarized Zone in Korea and hearing stories about what life is like in a place where every person must be ready to "Fight Tonight," to meeting cadets from the Texas National Guard's Texas Challenge Academy, who at age 16 to 18 chose to overcome challenges or face mistakes they had made and seize an opportunity for a second chance.

We got a (small) taste of the Marine Corps Crucible in San Diego and gained an appreciation for what it takes to make (or become) a Marine. We rappelled down the 64-foot tower with the Army National Guard at Fort Benning, Ga., and got to experience a gas chamber. We ate silkworms in Korea and Meals Ready to Eat in San Diego. I won't say which was better. We attended the 75th anniversary National Pearl Harbor Remembrance Day commemoration and watched Navy divers practice for an interment ceremony at the USS Arizona in Hawaii. We witnessed countless examples of what it means to be a leader in and in support of the United States military.

Amanda McGlone, Industrial Security Field Operations, helps set up a travelling Vietnam Wall exhibit in San Antonio, Texas.

Throughout the program, we spoke to leaders at every level of the chain of command, in every service, both civilian and military, and they all emphasized the importance of the same things – develop people, build strong relationships based on trust, strive for balance, leverage diversity, and be able to adapt to changing circumstances. What struck me was how critical their presence was to the reception of their message. They needed to communicate credibly in a balanced way for their message to be effective. Although all of the leaders communicated the same concepts, those who were seen as effective were the ones who clearly communicated how they applied those concepts. They made it clear they walked the walk and did not just talk the talk.

By far the most impactful part of the program for me was the ability to work closely and develop relationships with the 63 other participants in my cohort – highly motivated, exceptional individuals who are passionate about leadership and developing as leaders. Each member of the cohort challenged me and changed me for the better – a true marker of their leadership. From these relationships, I learned more about my own strengths and weaknesses in 10 months than I had in years prior. I learned how to leverage the diversity of people whose backgrounds and ideas are most different from my own to achieve outcomes greater than either of us had imagined possible. Failure and weakness are human and it is through experiencing and overcoming these that we became better as individuals and as a cohort. Through these relationships, I learned to leverage my hyper-competitiveness by reframing the competition

and seeing that we, DoD, are all on the same team. If one of us wins, we all win. Leadership is an art, not a science. There will always be more to learn, practice, and fine-tune.

Dustin Sievers

The 10-month ELDP utilizes leadership immersion and warfighter engagement to complement the academic and facilitated discussions regarding what it means to be a leader: in the world, in America, and within the enterprise. The lessons learned during this journey will stick with me for a lifetime.

The cohort consists of 64 high-performing civil servants and active-duty military personnel from across the DoD enterprise (talk about a networking opportunity!). You forge lasting bonds with the cohort members, each bringing their own experiences and perspectives to the table; many of the lessons learned are from each other.

To understand just how unique an opportunity ELDP is, try to think of another organization that operates on the scale, with the complexity of, or with the mission of the DoD; there is no other like it in the world! ELDP is an all-access backstage pass for you and 63? of your closest friends to explore just how the DoD enterprise is run; lessons and epiphanies abound!

While many in the cohort are already high-performers and competent leaders, ELDP has so many mechanisms to test and challenge each of us, it will unlock hidden talents you didn't know you had and help you identify areas to improve upon. You will have to face failure: how to cope, how to proceed, how to heal, and how to overcome fears all become tools to keep with you. Some of my own failures that I have learned from were not oriented on the execution of a task, but on the communication amongst my team members; my failure to communicate effectively resulted in a team failure.

ELDP gives you the tools to analyze leaders; their presence, philosophies, and the way they treat others are all open for discussion. Once you've found something that works, you can then try to incorporate it into your own leadership framework. Things that don't work, those toxic leadership traits, we're taught how to correct for.

In the process of self-actualization, I found myself changing my stance on a number of things. During our deployment to Texas, we met with Border Patrol, Customs and Border Protection, Texas State Troopers, and the Texas National Guard to learn about how they defend our southern borders. The trip re-framed illegal immigration for me and helped redefine my beliefs on what it means to be American. Since this trip, I have become an advocate for immigration reform, something I had never thought of before.

On each deployment in the 10-month journey, we were given multiple opportunities to engage with senior leaders. We're talking hour and a half one-on-one (or 64) sessions to pick the brain of four-star generals about leadership philosophies! What surprised me most about leadership philosophies at this level is that they are not complicated and are fairly simple in nature; taking care of people, building and maintaining relationships, and building the "next you" highlight the best philosophies I heard. The journey not only let me know exactly who I am as a person, but showed who I want to be.

I'm an advocate for continuous education and training, and the lessons within ELDP should be made available to everyone; almost as if it should be boot camp for all civil servants! If you're interested in such a journey, the best advice I can offer is to apply and be persistent. I didn't get in the first time or even the second; you've got to keep trying.

Dustin Sievers (right), Industrial Security Field Operations, stands in a Marine Corps Assault Amphibious Vehicle, at the Marine Corps Assault Amphibian School, Camp Pendleton, Calif.

Course covers topics that add complexity to industrial security program

By Garrett Speace
Morrisville Resident Office

Editor's Note: The following is a first-hand account of one DSS employee's participation in an industrial security course.

As the title implies, the "Applying Industrial Security Concepts" course focuses on the application of industrial security. While this is the aspect that industrial security representatives (ISR) traditionally spend most of their time focused on, the course also provided exposure to areas that are not common in the daily activities of an ISR.

The 16-week course, which serves as the culmination of industrial security training, builds on the foundation provided by the NISP Oversight course and the Managing Risk in Industrial Security course. The class consisted of ISRs from every region, bringing with them experiences unique to their geographic locations. But the common thread for all ISRs is the framework guiding the application of industrial security, the National Industrial Security Program Operating Manual (NISPOM). The NISPOM was written in a way that could be applied to security programs covering missiles in Colorado, aircraft carriers and submarines in Virginia, corporate headquarters in Washington, D.C., and electronic warfare in New Hampshire.

The course also focused on topics that tend to create complexity in a security program, such as foreign ownership, control, or influence (FOCI); foreign military sales, and arms, ammunition, and explosives. The greatest benefit to the course, however, was having the forum for ISRs to share their experiences, which in turn broadened each other's perspectives on ways to provide oversight and help implement effective countermeasures in industry security programs.

To close out the course, ISRs are required to complete a capstone project on a topic of their choosing. In the capstone, ISRs identify a problem in industrial security or in the operations of the agency, conduct research, and propose a solution. The process mimics that of developing new policy or a change in current operations, and requires the skill to advance these topics, such as communication, collaboration, tact and diplomacy, and

critical thinking. Many of these skills could be utilized in future positions should the ISRs move on to other roles such as field office chief, action officer, or regional director.

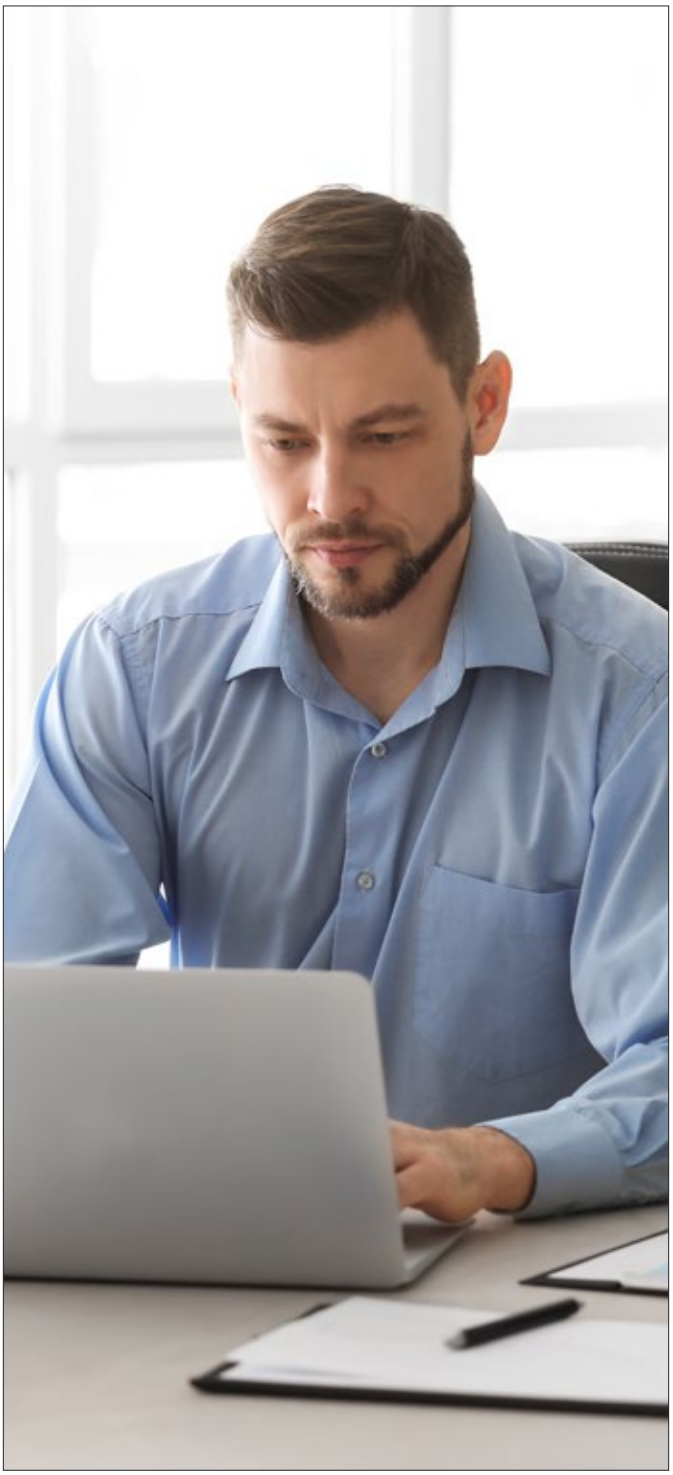
The class defended their capstones in front of two panels comprised of senior leaders from various directorates. The panels listened, asked sharp questions, and provided valuable feedback on what other information would be needed to strengthen the capstone/solution. The message that day from the panel members was to push on, continue with your ideas and "find their champion" -- someone who could assist the ISRs with pushing their solutions to the next level to create an impact and lasting change.

A lot of good ideas were presented to the panels but not all could be pursued by the agency. By finding a champion, the idea could be supported and promoted by others in the agency that have a need for the solution. The message to find your champion is not specific to any one position. It is advice that can serve anyone in any role. The course taught us to build our network as we all have good ideas and everyone needs help executing them.

The class selected six capstones to be considered by the Industrial Security Field Operations leadership. The topics consisted of succession planning for the field office chief position, improving the process for terminating facility security clearances, enhancing the review of COMSEC accounts, re-evaluating conducting assessments at homes, establishing a process for reintroducing employees from extended leave, and managing risk of overseas contractor operations. If selected for further development, these ideas could be implemented and have a positive impact on the agency.

Use resources available when establishing a risk-based security culture

by John B. Massey
Alexandria 2 Field Office Chief



Cleared industry is facing an unprecedented level of threat from foreign intelligence adversaries attempting to steal U.S. classified information and technologies for their own use. Adversaries use multiple and varying avenues of attack against cleared industry, prioritizing targeted information and shifting priorities based on their needs. When foreign adversaries are successful in obtaining this information, it damages national security, reduces the U.S. technological advantage and increases the risk to the warfighter. There has never been a more important time for cleared industry to establish risk-based security cultures within their organizations.

Understanding your facility's classified programs

The facility security officer (FSO) and security staff should understand the classified programs the facility is performing on, and getting this information comes from engaging with the contracts division, reviewing the DD Form 254, and knowing security classification guides. There are other items of information that are beneficial to security beyond these resources. Security should also consider engaging with program managers, engineers, and contract leads to truly understand classified operations at the facility.

Providing security education and training to your personnel

Cleared contractors are required to provide personnel with initial security training before they are granted access to classified information, and then annually thereafter. The National Industrial Security Program Operating Manual (NISPOM) requires this training to include: Threat awareness security briefing (including insider threat awareness), counterintelligence awareness briefing, overview of the security classification system,

employee reporting obligations, cybersecurity awareness training for all authorized information systems users, and security procedures and duties applicable to the employee's job.

Having a robust insider threat program

Effective May 2016, cleared contractors must establish an Insider Threat Program, which includes appointing an Insider Threat Program Senior Official (ITPSO), conducting insider threat training, and monitoring network activity. In addition, contractors are required to report insider threat information and conduct self-inspections annually that are certified by the senior management official.

For an Insider Threat Program to be both successful and robust, the ITPSO must have the authority to provide management, accountability, and oversight of the organization's Insider Threat Program and make resource recommendations to the appropriate organizational official. Successful Insider Threat Programs use auditing and monitoring, are supported by management, and include coordination and collaboration between multiple business pillars within the organization (i.e., security management, human resources, and business development).

Direct lines of communication with business development, human resources, program managers, and first and second line supervisors

Security personnel should be engaged with other elements within the organization. This includes engagement with

areas of the company that perform business development and human resources services. This engagement can ensure that other organizational elements are aware of methods of contact and operation that are used by the adversary when attempting to penetrate the organization.

Information sharing with government and industry partners

To establish a successful risk-based culture, facility security personnel should consider engaging with government and industry partners to develop an understanding of assets that employees are working on, why the assets are important to the U.S. government, and the threats and vulnerabilities to those assets.

Management engagement

It is essential that facility management be actively engaged in the security program. Senior management officials should have a keen understanding of the facility's operations and adversarial threats to programs they perform on. Management should also be informed of security matters and concerns that are prevalent at the facility.

Robust self-inspection programs

Contractors are required to review their security system on a continuing basis and must also conduct a formal self-inspection at intervals consistent with risk management principles. It is a best practice for security personnel to conduct continuous, ongoing self-inspections of security programs on site. These self-inspections should look beyond the NISPOM and consider identifying vulnerabilities not associated with a NISPOM citation.

Questions to Ask Yourself

When establishing a risk-based security culture, security personnel should consider asking themselves these questions:

- How would the adversary target my facility, personnel, and/or classified programs?
- What would the damage to national security be if the adversary was successful?
- Do I have a good understanding of the programs my personnel are performing on?
- Is senior management engaged and supportive of the security program?
- Does Business Development and Human Resources understand the nature of existing threats and information to be aware of that may place the organization at risk?
- Is adverse information reported via the Joint Personnel Adjudication System (JPAS) promptly?
- Are suspicious contact reports promptly provided to the DSS industrial security representative and/or counterintelligence special agent?
- Are employees knowledgeable of security practices and procedures?
- Do employees understand their reporting obligations?

Changing individual mindsets and fully engaging in all layers of a facility's operations is only the first step in establishing a risk-based security culture within your organization. In order to be successful, you must have a comprehensive understanding of your facility's programs, the threats to those programs, and the support of your organization's management.

RESOURCES:

There are several resources available to help you establish a risk-based security culture within your organization. The Center for Development of Security Excellence (CDSE) offers a variety of case studies, job aids, and training courses available for industry (www.cdse.edu).

The DSS Counterintelligence Directorate releases the unclassified publication, "Targeting U.S. Technologies: A Trends Analysis of Cleared Industry Reporting." The report analyzes suspicious contact reports received from cleared industry and is available on the DSS website (www.dss.mil).

DSS field offices host monthly secure video-teleconferences for cleared industry. CI special agents are also available to provide threat briefings to employees at your facility. Contact your DSS industrial security representative or CI special agent for more information.

Andover Field Office partners with industry, government

by Kathryn Kimball
Andover Field Office

The Andover Field Office hosted its 4th Annual Partnership with Industry Day on Sept. 20, 2017. Collaboration between field office personnel, DSS leadership, the Personnel Security Management Office for Industry (PSMO-I), Northern Region staff, Counterintelligence (CI) and Cyber Operations made the event a huge success.

The number of participants more than doubled from the previous year, as close to 200 industry security professionals representing 114 different cleared contractors from Massachusetts, Maine and New Hampshire attended the event at Hanscom Air Force Base, Mass. In addition to industry, 10 government security professionals from the 66th Air Base Group at Hanscom attended along with four representatives from two Federally Funded Research and Development Centers.

The day-long event, orchestrated by Industrial Security Representative Clement LaShomb, provided relevant National Industrial Security Program information and guidance to industry in a collaborative environment. Gus Greene, director, Industrial Security Field Operations, introduced the new DSS methodology to industry by discussing the four primary components: Prioritization; Asset Identification; Threat – Vulnerability - and Impact Assessment (TVI); and Tailored Security Programs.

Other topics on the agenda this year included presentations from PSMO-I and DSS CI, who discussed adversary business ethics and current cybersecurity trends in industry. The New England Chapter of the National Classification Management Society discussed the state of NCMS. Additionally, a break-out session was held on implementation of the Risk Management Framework for information systems security managers/information systems security professionals.

The day concluded with a panel of DSS subject matter experts answering questions from the audience.

Andover Field Office hosted its 4th Annual Partnership with Industry Day.

Quotes from industry participants:

"

Keep these events coming!

All of the presentations were very beneficial. I learned the most from the cybersecurity presentation as I had very little knowledge on this topic.

The DSS in Transition briefing was exceptional! Mr. Greene's time spent with us was tremendously valuable.

No recommendations – **you covered a wide band of subjects** and I think you did it **very well**.

"

Targeted FOCI training provides techniques to address risk during SVAs

by LaHoma Kotchian
Region Action Officer, Western Region

While the Industrial Security Integration and Application (ISIA) directorate is responsible for emplacement of the proper action plan to mitigate foreign ownership, control or influence (FOCI), the Industrial Security Field Operations (IO) directorate is responsible for oversight of the cleared company and its compliance with that action plan. The Western Region recognized a distinct need for formal training and developed a plan to empower its field personnel with an understanding of FOCI mitigation and techniques to conduct skilled FOCI oversight.

In July 2017, Western Region hosted 16 industrial security representatives (ISRs) and information systems security professionals (ISSPs) with cognizance over FOCI companies for targeted FOCI security vulnerability assessment (SVA) training in the Cypress Resident Office. Using a FOCI oversight presentation as a foundation, Western Region Action Officers LaHoma Kotchian and Curtis Peay revamped that presentation, fleshed it out into several modules, and conducted the formal three day training. The training team received valuable expertise and input from Matt Blakley, Regional Operations Manager, Southern Region, who created the original presentation, as well as Action Officers Michael Pilla (Northern Region), Brian Murphy (Southern Region), and Shobha Ramaswamy (Capital Region).

Class Photo: **FRONT ROW** (from left): April Rodriguez-Plott, LaHoma Kotchian, Nadja West; **SECOND ROW**: Juaquita Gray; **THIRD ROW**: Maya Rudela, Richard Owens, Sam Losee, Juan Carrillo; **FOURTH ROW**: Miranda Johnson, Renee Farris, Thomas George; **FIFTH ROW**: Jared Ostertag, Monica Son, Duane Shannon, Jerry Ousley, Derek Sinclair; **BACK ROW**: Curtis Peay

The primary objectives of the training were to ensure field personnel fully understand the purpose of FOCI mitigation (the "why") and to learn the tactics, techniques, and procedures to properly address risk during SVAs at FOCI signatories (the "how"). Topics included an overview of FOCI and FOCI action plans (from emplacement to compliance); preparing for the SVA; reviewing and overseeing supplemental plans, such as electronic communications plans, affiliated operations plans (AOPs), facility location plans, and technology control plans. There were also sessions on conducting the signatory SVA and writing the FOCI SVA report. Southern Region personnel provided an overview of FOCI case studies and Maria Ong, IP Mitigation Strategy unit, provided an overview of the AOP, the approval process, and how to provide oversight for the plan; both via video teleconference. Western Region Counterintelligence (CI) Deputy Chief Jeff Boick discussed how to approach a FOCI SVA from a CI perspective.

The training was largely a lecture format in an informal setting, but the participants were also given hypothetical case studies in which they were asked to work in group settings to analyze the cases in depth and come up with viable solutions. Participants also shared best practices and explored methods of effectively using integration (across three directorates: IO, IP, and CI) during team assessments. Plans are to use this in-depth training as a springboard to assist DSS personnel in other regions by building upon it and replicating it in the future. The team also led to the creation of a FOCI glossary which includes the unique terminology of the FOCI arena. The goal is to turn the glossary into an approved job aid.

'One thing you can't change is change; embrace the change'

by Dahlia Thomas
Industrial Security Field Operations

Senior Industrial Security Specialist Bill Blevins.

They say the only constant in life is change. Bill Blevins can certainly attest to that idea having seen his share of change in his 35 years at DSS. Currently a senior industrial security specialist, Blevins started his career as a mail clerk and motor vehicle operator at the Defense Investigative Service, the precursor to DSS, on Sept. 5, 1982. He came to the agency shortly after graduating from Woodbridge Senior High School and worked his way from a GS-3 to his current position as a GS-13.

Looking back, he never imagined the many changes he would see in technology and the security profession over the years. For instance, he saw computers transform from IBM Display Writers using 12-inch floppy disk drives, to tablets with a smaller footprint than those 12-inch drives. He saw pagers and bulky cell phones give way to sleek, multi-functional smart phones that you carry in a pocket. And, he is now witnessing the transformation of the agency mission from a focus on compliance with the National Industrial Security Program Operating Manual to a focus on identifying and mitigating risk through the DSS in Transition initiative.

Throughout his 35 years, he adopted the phrase, "One thing you can't change is change. Embrace the change. Live it, love it, learn it." He recognized how new technology was introducing new threats to national security through cyberspace. Blevins recalled mentoring Karl Hellmann, the current NISP Authorizing Official, as one of those security professionals that he helped along the way. Hellmann said, "Having known Bill since I first started with DSS, I have always considered his dedication to the DSS mission as exemplary. Bill has always been one to share his knowledge and experience with all. Over the years he has improved and assisted both DSS employees and industry in security matters under the NISP. We will miss his commitment and friendship as he moves into the next chapter of his life."

DSS employee retires after 36 years of federal service

Senior Industrial Security Representative Gary S. Layne of the Virginia Beach Field Office retired in June after 36 years of federal service. Layne began his federal career in August 1980 as an intern computer specialist for the Department of the Navy, and while in college, he interned during his summer and winter breaks. He joined the Defense Investigative Service (DIS) in 1985 as a special agent, background investigator, until he became a DIS polygraph examiner in 1991. Layne left the polygraph profession and became a DSS industrial security representative eight years later. He was promoted to senior industrial security representative in 2006, and since then has trained many of the other industrial security representatives in the field office.

"Gary was a valued member of the Virginia Beach Field Office and the Southern Region," said Beth Whatley, Virginia Beach Field Office Chief. "He used to always say that when someone leaves, their coworkers miss them for a while and then things just keep moving on without them. I can honestly say in this case, he was so wrong! All of us miss Gary's energy, leadership and commitment to always going the extra mile for his contractors and his teammates."

Regina Johnson (left), Southern Region Director, presents Senior Industrial Security Representative Gary S. Layne, of the Virginia Beach Field Office, his retirement plaque during a ceremony recently.

My journey: From intern to industrial security representative

by Alyssa Dittrich
Virginia Beach Field Office

Editor's Note: The following is a first-hand account of one DSS employee's transition from being a student intern to an industrial security representative.


Alyssa Dittrich

My journey with DSS started in the summer of 2016. I was one semester into graduate school and very proactive in preparing my coffee making skills as a soon to be intern. For background, I grew up all over the world as the daughter of a United States Marine, I am a proud spouse of a United States Airman who deploys more than I would like, and I am working on my master's degree in homeland security with a focus in counterterrorism. Adaptation and change are things that come easily to me, which is why national security and the protection of our warfighters is not only my life mission, but also my passion. However, what I did not realize then was that taking an internship in the Virginia Beach Field Office would be the best decision of my professional life.

Anyone with my academic major will tell you that finding a job or internship in this field can be very difficult and extremely competitive. So when my husband's civilian coworker told him about the DSS internship, I searched immediately and discovered I had one day to apply. I put together whatever I could possibly find to land this internship...and I did.

On my first day in the office, my expectation of admin type work went out the window. This was definitely going to be a hands-on and completely interactive internship. Immediately my calendar filled up with security vulnerability assessments (SVA) and sitting on my desk was a big binder, labelled "NISPOM." My mentor, Susie Miller, is tough, to the point, and always willing to help you reach your goals. Instead of talking at me about the processes, she took me on my first SVA. Every step she took, I took. When I didn't understand something, she immediately explained it – sometimes without my ever asking.

Like everyone else in the agency, our office is always busy. Not only did I experience the different challenges and jobs of the field with my mentor, I also experienced them with everyone else. The people in this office and their encouragement are why I continued as an unpaid intern when the summer was over. I knew that I wanted to be part of this agency no matter how long it took. I stayed not because I wanted a job, but because I loved this job. I attended over 170 SVAs during my internship, I witnessed the good, bad, and ugly and I still loved the job. I attended RED DART conferences, countless NCMS meetings, the 2016 DSS All-Hands, and even an event we held to meet all of our local government contracting activities. I have been here through the shift to DSS in Transition and experienced our office's strategies for implementing a risk-based, asset-focused, and threat-driven approach to security. When a position opened up, I gave it everything I had to officially be part of this team as a full-time DSS industrial security representative... and I got the job.

A year and a half ago, I never dreamed of being where I am now. Though this agency is constantly changing, the world is continuously evolving, and our office looks nothing like it did a year ago but our mission as a whole has always remained constant. I am surrounded by a loving, intelligent, and dedicated group of people. I am proud to have found a career where I know what we do truly makes a difference to national security. This job gives us the chance to give back to our nation's warfighters, which hits home for me because it is those men and women who have given me everything in my life. I am excited to come to work every morning and learn something new. I enjoy researching and expanding my knowledge on how to improve our capabilities as industrial security representatives. The collaboration and family-oriented relationship between my colleagues and me make my job so much more enjoyable than I ever could've imagined. I can't wait to see where my journey with DSS takes me next.

O'er the Ramparts We Watched:

Capital, Northern Region Counterintelligence teams explore history, leadership competencies during staff ride

by Allison Carpenter, *Counterintelligence, Northern Region,* and **Michael Clapp**, *Counterintelligence, Capital Region*

Winston Churchill said, "The farther backward you can look, the farther forward you are likely to see." To cultivate their leadership skills, the Counterintelligence Field Operation staffs from the Capital and Northern Regions explored military and civilian leadership styles in the War of 1812 during a leadership development staff ride to Fort McHenry in Baltimore, Md., earlier this summer.

While staff rides are new to DSS, they have long been used in the military to teach leadership concepts. Fred Bolton, DSS Leadership Development Program manager, kicked off the event at the Center for Development of Security Excellence in Linthicum, Md., with a group discussion on the history of the war, the tactical logistical and operational decisions made by American and British leaders from 1813-1814, and battlefield strategies used by both sides.

The groups discussed an 1813 British tactical decision to fight another war front in the mid-Atlantic, hoping to disrupt American forces engaged with Britain and her allies on the Canadian border. Additionally, the DSS regional leaders and employees discussed the impact of American politics and their involvement in battlefield decisions. Before leaving the classroom, Bolton challenged the CI teams to identify DSS leadership competencies demonstrated from the beginning of the Chesapeake Campaign in Upper Marlboro, Md., to the successful American defense of Baltimore while participating in the staff ride.

The groups then traveled to Fort McHenry National Monument and Historic Shrine where they examined U.S. soldiers' life at the fort, and the defense of Baltimore. The Battle of Baltimore, September 12-14, 1814, is one of three times since the American Revolutionary War that the United States was attacked on home soil by foreign forces. The British Navy bombarded the fort for 25 hours, but failed to force the Americans to surrender. As the British fleet withdrew down the Patapsco River, the garrison flag, now known as the Star-Spangled Banner, was raised over Fort McHenry, replacing the smaller storm flag that flew during the bombardment. A storm flag is a smaller flag that is usually hung when there is a storm over the military post. During the visit to Fort McHenry, the Capital Region CI special agents were selected to lower the storm flag and raise the garrison flag at 10 a.m. This is historically significant because that was the same time that Major George Armistead, Fort McHenry commander, ordered the garrison flag raised to signal American victory in the defense of Baltimore.

After leaving Fort McHenry, the group returned to CDSE where Bolton provided an analysis of the battle, and the group broke into teams to discuss the elements of leadership revealed during the campaign. As Bolton indicated, "a key part of a successful staff ride is to reflect on the events that occurred in the past and link them to current challenges and key leadership competencies at DSS. Leadership under stress is a constant theme in the past, as well as the present since war has a constant nature, but an ever-changing character."

The team cited communications, respect, integrity, agility, collaboration and accountability as key themes between the leadership during the campaigns and the current environment at DSS. By looking back at history, the staff ride participants were able to look toward the leadership competencies, which are the basis for the new DSS Leadership Development Program.

CI special agents from the Capital Region took part in the flag ceremony at Fort McHenry National Monument and Historic Shrine.