DSS ACCESS

Official Magazine of the Defense Security Service | **Volume 5, Issue 1**

New training provides opportunity to apply complex decision-making, risk-management skills

DSS ACCESS

Published by the
Defense Security Service |
Public Affairs Office

27130 Telegraph Rd.
Quantico, VA 22134

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

DSS LEADERSHIP

Acting Director | James J. Kren

Chief of Staff | Troy Littles

Chief, Public Affairs | Cindy McGovern

Editor | Elizabeth Alber

Graphics | Steph Struthers

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.

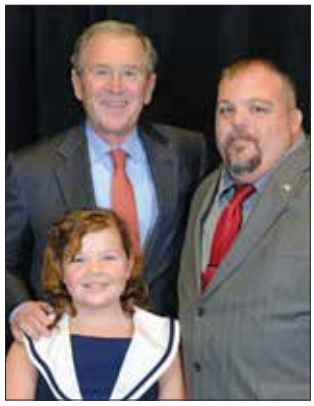
The views expressed by the authors are not necessarily the official views of, or endorsed by, the U.S. Government, the Department of Defense, or DSS.

All pictures are DoD photos, unless otherwise identified.

COVER

INSIDE

ASK THE LEADERSHIP



THE ENEMY WITHIN

AROUND THE REGIONS

From the Acting Director

What a time of change and opportunity for DSS! In early January, we bid farewell to Stan Sims, DSS Director for the past five years. We achieved incredible success over his tenure, and he left the agency a strong foundation on which to continue to build and move DSS forward. Just before going to publication on this issue, it was announced that Dan Payne was selected as the new director. Dan is well known and respected within the counterintelligence and security community and has been a friend and supporter of DSS.

Dan is currently the Deputy Director of the National Counterintelligence and Security Center. He is a career counterintelligence officer with the Central Intelligence Agency who has spent more than 30 years in the field of counterintelligence. Dan joined the National Counterintelligence and Security Center from a position at CIA as a Deputy Chief of South Asia Division. Dan's previous senior assignments at CIA include Deputy Chief, Counterintelligence Center; Assistant Inspector General for Investigations; Deputy Director, Counterterrorism Center for Counterintelligence; and Deputy Chief, Counterespionage Group.

I believe Dan will find DSS is a "lead agency" — that we are an agency focused on our mission, our fundamental principles and well rooted in our Strategic Plan. Our strategy roadmap clearly outlines where we must continue working together to strengthen our capabilities to identify, evaluate and mitigate risk; enable our stakeholders to proactively manage risk; strengthen national security partnerships; empower our mission-driven workforce; and provide enterprise solutions. Every DSS government and contractor professional has a key role, and everyone's contribution will be needed going forward.

I am honored to have served in an acting capacity and look forward to a smooth leadership transition. I know that you will extend to Dan the same support and dedication that you have given to me and Mr. Sims. Please join me in welcoming Dan and making him a part of the DSS family.

Thank you for all you do.

Jim Kren
Acting Director

New training provides opportunity to apply complex decision-making, risk-management skills

by Heather Mardaga
Center for Development of Security Excellence

When the Center for Development of Security Excellence (CDSE) released three new courses in October 2015, it expanded the initial training of industrial security representatives to promote the development of industrial security subject matter experts.

The three courses, designed exclusively for industrial security representatives, are the National Industrial Security Program (NISP) Oversight, Managing Risk through Industrial Security, and Applying Industrial Security Concepts.

The courses came about as the result of a training needs analysis for full performance industrial security representatives done in September 2011. The analysis revealed the need for in-depth training in the areas of critical-thinking, higher-order analysis, problem-solving, and evaluation. Based on that recommendation, a comprehensive curriculum was created to provide the opportunity to apply complex decision making, risk management and high-level communication skills to complex situations similar to those that full performance industrial security representatives would encounter in the field.

Collectively, these three courses establish a new, unique developmental career path. They provide students with opportunities to complete case studies, and apply critical thinking and risk management principles to various levels of complexity. The courses also promote the standardization and consistency of policy implementation across DSS. Below are the descriptions for each of these three courses:

NISP OVERSIGHT

Six-month virtual instructor-led course that allows new industrial security representatives (IS reps) to demonstrate knowledge and skills to independently conduct both initial facility clearance actions and low-to-medium risk Security Vulnerability Assessments.

In this course, students work both within their field offices, as well as participate in live class sessions where they have opportunities to collaborate with other new IS Reps to complete assignments and present to DSS subject matter experts.

MANAGING RISK THROUGH INDUSTRIAL SECURITY

Four-and-a-half-day instructor-led course that allows IS reps to apply and demonstrate technical knowledge and skills to independently react to challenging NISP oversight situations.

In this course, students work through real-life case studies and apply critical thinking and risk management principles to identify possible solutions. Students have multiple opportunities to collaborate with other IS reps when analyzing the case studies for potential risks and brainstorming possible mitigation solutions.

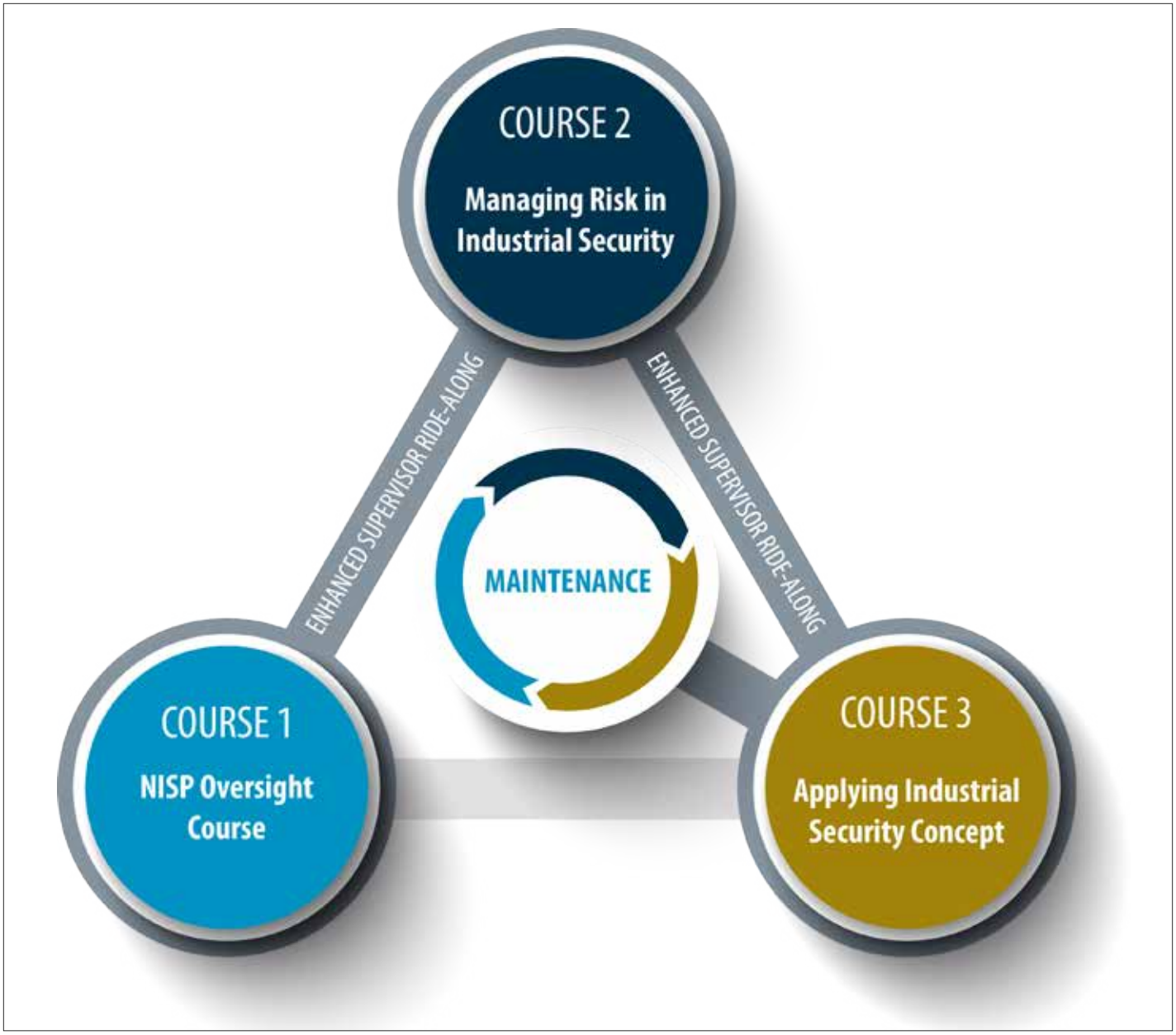
APPLYING INDUSTRIAL SECURITY CONCEPTS

Sixteen-week virtual instructor-led course with a three-day instructor-led capstone for IS reps to apply higher-order skills to complex NISP oversight situations.

In this course, students work on a capstone project where they identify and investigate a real-world DSS or industrial security problem, conduct an investigation, and make recommendations via written report and oral presentation to DSS leadership during a three-day visit to DSS headquarters.

During the design process, CDSE and Industrial Security Field Operations collectively agreed that industrial security representatives must have a voice early on in the training development process to create premier training. To accomplish this goal, CDSE led multiple design meetings in November 2014 with more than 20 industrial security representatives participating.

In addition, subject matter experts from Industrial Policy and Programs and Counterintelligence collaborated on the design and content of the courses and ensured the courses met DSS field personnel's expectations. The design team also acknowledged that courses would need to be designed using various platforms to reach all the IS reps across the nation. As a result, a virtual instructor-led platform was leveraged for two of the



courses, while also designing collaborative learning opportunities within the course.

Between July and November 2015, CDSE conducted beta tests for the three courses. When asked what they liked most about the course, many participants mentioned the interactivity, collaboration, and content. Participants stated:

> "[Managing Risk through Industrial Security] didn't feel like 'death by PowerPoint'. It was **much more interactive** than I thought it would be.

> "[Applying Industrial Security Concepts]'s weekly assignment topics **greatly enhanced my knowledge base** applicable to my role as [an] ISR.

They also enjoyed the opportunities for group interaction and collaboration that were built into the courses. Other participants commented they wished they had received this training six years ago when they first started with DSS.

Over the next fiscal year, CDSE will offer multiple iterations of these new courses in order to meet the ongoing demand.

DSS bids farewell to agency director

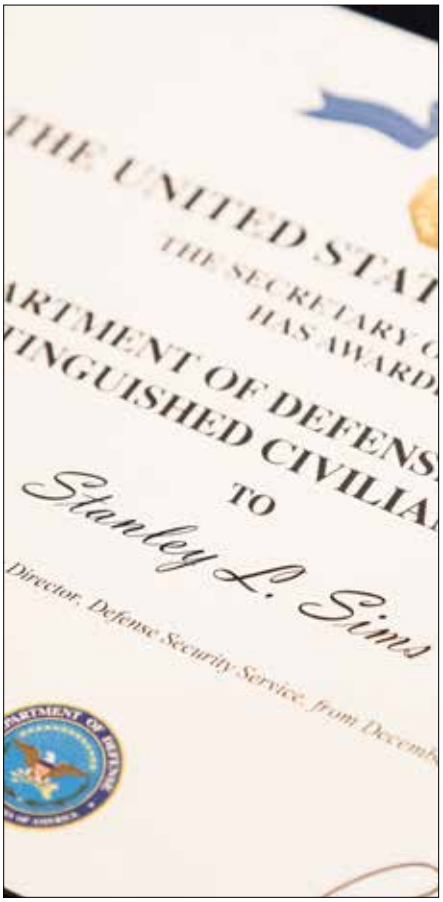


PHOTO PAGE

TOP: An audience of senior DoD and government officials, industry partners, family, friends and the DSS workforce filled much of the Marine Corps Base Quantico theatre for the retirement ceremony of former DSS Director Stan Sims. *(Photo by Hollie Rawl, CDSE)*

BOTTOM LEFT: The Marine Corps Base Color Guard presents the colors during the retirement ceremony for former DSS Director Stan Sims. *(Photo by Marc Pulliam, CDSE)*

BOTTOM MIDDLE: At his retirement ceremony, former DSS Director Stan Sims reacts to the opening remarks by Under Secretary of Defense for Intelligence Marcel Lettre. *(Photo by Hollie Rawl, CDSE)*

BOTTOM RIGHT: Under Secretary of Defense for Intelligence Marcel Lettre presented former DSS Director Stan Sims with the Department of Defense Medal for Distinguished Civilian Service. The DoD award recognized Sims' "extraordinary leadership and strategic vision, which enabled DSS to deliver exceptional support to 26 Department of Defense components and 30 federal agencies." *(Photo by Hollie Rawl, CDSE)*

The Defense Security Service bid farewell to Stan Sims, the agency's 12th director, in a retirement ceremony in early January. The event reflected on Sims' government career, his tenure at DSS and the role of the agency in national security. The audience, which included senior DoD and government officials, industry partners, family, friends and the DSS workforce, filled much of the Marine Corps Base Quantico theatre.

Officiating at the event was Under Secretary of Defense for Intelligence Marcel Lettre. In his opening remarks Lettre said, "What we celebrate today is an organization that for 44 years has quietly been the foundation of the Department of Defense's personnel and industrial security enterprise. We are also celebrating a true American patriot in Director Stan Sims, who has ably led this fine organization since arriving on December 5, 2010, as the twelfth DSS Director and is culminating 36 years of distinguished government service."

Lettre noted the agency's personnel security origins, its changing mission over its history, and its current operating environment, "Given the challenges of protecting such information in today's high-tech world, DSS' success in this arena is nothing short of extraordinary," said Lettre. "I know Stan has said this numerous times — and I will repeat it here — in so ably handling this complex mission, DSS is lifting well above its weight."

In looking back on Sims' tenure and legacy, Lettre said, "Under Stan's leadership, DSS made integration and cooperation not just a bumper sticker but a way of life. Stan is a strong believer in the value and necessity of a single, cohesive national-level industrial security program. Successful execution of the National Industrial Security Program demands cooperation at multiple levels ... within the Defense Intelligence Enterprise ... across governmental agencies ... and most critically between industry and government. His team has broken down internal silos, but more importantly has built real trust between government and industry."

Lettre acknowledged Sims' contributions to the agency's mission, but also cited Sims' focus on and care for the DSS workforce. "First and foremost he demanded pride in ourselves ... in the DSS mission ... and the organization. The pride is now felt throughout the organization ... and because of that pride — and a tremendous amount of hard work and dedication — DSS has earned respect for the agency and its workforce throughout the interagency security community. This is evident by the diverse and prestigious audience in the room today."

Lettre addressed the agency workforce as well as its government and industry partners and the role they play in national security. "To the entire DSS team — thank you for all you have done to support Stan during his tenure as director. More importantly, thanks for the blood, sweat, and tears that have made DSS a symbol of excellence, and that have positioned DSS strongly for a turbulent security environment in the future. You are a small agency, but a tough agency, an elite agency. You are at the forefront of responding to our nation's trickiest security challenges — countering foreign industrial espionage, hardening industry against cyber intrusions that steal our intellectual property, protecting our industry against insider threats. I want you to know how much I appreciate what you do."

"To our government and industry partners," said Lettre, "I think we share the view that success in protecting our great nation lies in cooperation and partnership. We need a coordinated, integrated approach that maximizes resources as we solve today's wicked problems. Our industry partners are our nation's economic engine, ensuring a prosperous America, a capable military, and in turn a secure America. To our government partners, please know that the DSS is a valuable asset for your organizations and does a fantastic job representing you and your interests. Please continue to partner with them."

In closing, Lettre addressed Deputy Director Jim Kren, now Acting Director, and charged him with "exercising fully all the leadership responsibilities necessary to keep this strong organization moving forward."

Lettre said the process is under way for the Secretary of Defense to make a final selection for the new director, but that it would take time to ensure the correct person was selected. "In the meantime, you will lead this organization admirably, and I know the team you have around you — the senior leaders, and the hundreds of talented people across the DSS team — will lean in to the job of continuing to make sure DSS is strongly positioned to deliver on its mission."

Following his remarks, Lettre presented Sims with the Intelligence Community Seal Medallion on behalf of James R. Clapper, Director of National Intelligence, who was unable to attend.

He also presented Sims with the Department of Defense Medal for Distinguished Civilian Service, a Senior Executive Service flag and retirement letter from the Secretary of Defense.

The DoD award recognized Sims' "extraordinary leadership and strategic vision, which enabled DSS to deliver exceptional support to 26 Department of Defense components and 30 federal agencies as part of its mission to administer the National Industrial Security Program on behalf of the Secretary of Defense."

Sims thanked his mentors from his earliest days as an Army officer to his current position. "As I look out over the audience," said Sims, "I am humbled and touched by the fact that so many of you took a pause in your busy schedules to simply be here today — to help make this day so very special for me and my family … All of you have helped me, supported me, made sure I would not fail throughout my military and federal service career — and there are so many more."

In his final remarks to DSS, Sims said, "What you do for our nation is unique in the U.S. government and our government depends on you to perform this unique mission. You are a national asset. What you do for our collective security — there is no one better at it than you. And while faced with many challenges … you always pressed forward through those challenges — because it was the 'right thing to do!'"

Mr. Sims concluded by telling Mr. Lettre, "Mr. Secretary, I leave you with the confidence that the National Industrial Security Program is in good hands."

Dr. John Hamre, President and Chief Executive Officer of the Center for Strategic and International Studies, and former Deputy Secretary of Defense, asked that a letter addressed to Sims be read at the retirement ceremony:

"

… I feel a personal sense of responsibility for the difficult trajectory that DSS has experienced the past 20 years. When I was the comptroller for the Defense Department, we imposed very deep cuts on DSS.

It was a time when all of the department was undergoing steep declines, but we certainly pushed very deep cuts on DSS. It was only later I came to appreciate the important work of DSS for the department and the country.

… You can look back on your tenure as director of the Defense Security Service with pride and a well-earned feeling of accomplishment.

Your life journey will take you in new directions, but I know your heart will always be with the men and women of the Department of Defense whom you have served with such high distinction.

"

Outgoing DSS Director holds final town hall

TOP: Former DSS Director Stan Sims provides an update on DSS initiatives during the DSS town hall. | **BOTTOM:** Jeff Cavano (left), Industrial Policy & Programs, take notes during the town hall, while Micah Komp, Industrial Security Field Operations, listens. *(Photos by Marc Pulliam, CDSE)*

Stan Sims, outgoing DSS director, made holding a town hall meeting with agency employees an annual event where he articulated his vision for the agency and reported on the agency's successes and challenges.

In his final town hall, held in December 2015, Sims returned to the themes he articulated at his first town hall of January 2011.

Sims said, "I had one simple goal when I stepped into this job and that was to leave the agency better than when I arrived. In the first couple of days, I had to decide how to achieve my goal."

Sims' strategy for achieving his goal was three things:

- People first, mission always;
- Partnership with Industry; and,
- Telling the DSS Story.

In terms of "people," Sims cited the new hiring process, Director Awards program and organizational pride as examples of how the culture at DSS had evolved and changed. In terms of partnership, Sims noted the change from a compliance based inspection regimen in Field Operations to a risk based assessment regimen. He also noted the enhanced sharing of threat information with cleared industry as another example of the strengthened partnership.

"I hope you embrace that as how DSS does business," he said. "Continue to improve the partnership with industry, use your authority a different way."

Sims said he embraced telling the DSS story because he knew there were many on the staff at the

Office of the Under Secretary of Defense for Intelligence who didn't know what DSS was doing. "I knew you were doing good, thoughtful work," he said. "The problem was you weren't telling your story and you weren't being recognized for that work."

Examples of telling the DSS story included the successes at the Center for Development of Security Excellence, cyber accomplishments, analysis of Foreign Ownership, Control or Influence and automation initiatives.

"We have the most security experts in DoD and are the only security organization in DoD, and quite possibly the federal government. We're it. We are the experts whether we think we are or not. It's part of our story and we are good at what we do," Sims said.

While Sims cited many accomplishments during his tenure at DSS, he said he was leaving with several goals left undone, to include manpower resources and a leadership development program.

"Our numbers are actually smaller than we were five years ago. I can't get people to understand that a small investment in DSS leads to huge returns to national security," he said.

Another goal left undone is a leadership development program. "Leadership matters," Sims said. "The goal should be to make better leaders. The leadership development program is working but it won't solve everything and it must continue to evolve and grow."

In closing, Sims said his time at DSS was the longest of his entire professional career. "People ask me, what made me stay so long? It was you. Transition is normal for me and I'm not bothered by transitions but I am bothered by leaving the people. You are a devoted group of people and you have done everything I asked you to do for the small amount we pay you. You are a very committed group of people and I am amazed at the energy you put into your jobs. I appreciate your support and willingness to follow me."

DSS welcomes new **Chief of Staff**

In early December, DSS hosted a promotion ceremony and formally welcomed Troy Littles to the position of Chief of Staff. Littles, who was promoted to the Defense Intelligence Senior Executive Service (SES), had previously served as the Director's Executive Officer.

In his remarks, Stan Sims, DSS Director, said the essence of an SES was the ability to lead and the key selection criteria for any SES. "It's what makes Troy uniquely qualified to serve as Chief of Staff," said Sims. "He has demonstrated leadership throughout his military and civilian career."

> "It's what makes **Troy uniquely qualified to serve as Chief of Staff**," said Sims. "He has demonstrated leadership throughout his military and civilian career."

Littles began his military career as a private first class in the United States Marine Corps Reserve. He eventually transferred to the Longwood College Army Reserve Officer Training program where he graduated and was commissioned as an infantry officer.

Over the next 26 years he held numerous positions of increased responsibility in Korea, the United Kingdom, Saudi Arabia, and Iraq, culminating with a deployment in support of Operation Enduring Freedom in Kabul, Afghanistan, and retiring as the chief, Information Operations Division, North American Aerospace Defense Command/United States Northern Command.

After retirement, he became the chief, Operations & Intelligence Support Division, United States Army Space & Missile Defense Command & Army Forces Strategic Command (USASMDC/ARSTRAT), where he was responsible for providing timely, accurate, and relevant current and operational intelligence analysis, security, counterintelligence, all-source collection management, exercise intelligence, and combat development support to USASMDC/ARSTRAT senior leaders.

ABOVE: New DSS Chief of Staff Troy Littles (center) and former DSS Director Stan Sims (right) watch as Timothy Harrison, chief of DSS Security, unfurls the Senior Executive Service flag. *(Photo by Marc Pulliam, CDSE)* | **AT LEFT:** New DSS Chief of Staff Troy Littles (left) receives the Senior Executive Service pin from his wife Karen Littles. *(Photo by Hollie Rawl, CDSE)*

Sims cited the role of the Chief of Staff in DSS — not only does the individual supervise the agency's staff offices; it also serves as the link between the staff, the mission directorates and the director.

"There is no other position in the agency that has insight and a view into each area. It truly is the keystone of the agency," said Sims. "That's why Troy is uniquely suited to serve as Chief of Staff; because he understands this. He already has that insight and more importantly, he has the trust and respect from each of those components."

CDSE recognized for continued innovation in distance learning technologies

The Center for Development of Security Excellence (CDSE) received a Federal Government Distance Learning Association (FGDLA) Five-Star Award at a ceremony in Washington D.C., on Dec. 2, 2015.

The award recognizes CDSE's continued innovation in distance learning technologies including eLearning courses, virtual environment delivery, performance support tools, webinars, and the CDSE YouTube Channel. CDSE was previously recognized as a Five-Star Award winner in 2013.

The FGDLA is a professional association that supports distance learning in the federal government. Its main goals include facilitating, guiding, developing, leading, and advocating the use of distance learning for training and education. CDSE was one of eight agencies to receive the award for its support of distance learning.

As video technology has continuously evolved and become increasingly available on mobile devices, video production has been interwoven more tightly into CDSE's distance learning strategy, and various learning and marketing products over the course of several years.

Since its establishment, the **CDSE YouTube channel has had over 80,000 views**, and viewers have watched an estimated 328,101 minutes of videos.

In response to the needs of DoD and industry security personnel, CDSE has created videos focused on specific topic areas for over seven years. One of the most viewed videos, with more than 11,500 views, shows how to operate and close a combination lock, as well as changing lock combinations.

The CDSE YouTube Channel broadcasts archived webinars and videos for security training, education, and certification. It was first established in 2011 and houses approximately 60 videos for the security community to access 24 hours a day, seven days a week. Since its establishment, the CDSE YouTube channel has had over 80,000 views, and viewers have watched an estimated 328,101 minutes of videos.

All videos are produced by CDSE and address a range of security content areas, including counterintelligence, cybersecurity, information security, industrial security, personnel security, and physical security. Besides addressing these areas, the videos vary in purpose. Some demonstrate how to use a system or device while others convey information or provide examples of how to interpret policies.

In 2013, CDSE launched an initiative that uses videos to help viewers become acquainted with CDSE course material. Additionally, videos of this nature are used within several graduate-level distance learning courses to give students an opportunity to see their instructors speak, as if they were meeting them in a face-to-face classroom setting. The CDSE website also showcases videos inviting viewers to engage with CDSE products.

On Sept. 25, 2014, CDSE hosted its inaugural virtual conference to over 1,000 registered civilian and military personnel from around the globe. Due to budget and travel constraints, the DoD Security Conference had been on hiatus since 2011; however, by using a collaborative online platform that included the use of webcam videos and audio through telephone or voice-over internet protocol, CDSE was able to provide the security community a comparable conference experience.

All sessions were recorded and posted for registrants to view as needed. Helpful features such as bookmarking and search capabilities were implemented to help viewers quickly navigate the videos to find needed information.

Leveraging the success of this model, CDSE hosted a live 2015 DoD Security Conference and offered several live streaming sessions to virtual participants, including video with closed captioning.

Attendance numbers at the 2015 DoD Security Conference further illustrated the invaluable impact of video use for DoD security professionals unable to attend in person. Virtual attendance exceeded in-person attendance with approximately 700 viewing virtually and 300 onsite. Virtual

2015 DoD Security Conference attendance included over 700 personnel participating virtually from across the Federal Government, logging in from as far away as South Korea, Japan, and Rwanda.

attendees greatly appreciated the ability to participate, since barriers such as budget cuts, travel constraints, and shortage of manpower prevented attendance in person.

Released in May 2015, an onboarding refresher 15-minute video is designed for DSS managers and supervisors to help them continue the onboarding process of new employees during their first critical six months of employment. The video delivery format provides a portable, efficient, and standardized method of demonstrating roles and responsibilities of managers and supervisors during the formal onboarding and integration process.

Leaders in the DoD community have seen positive results after using CDSE videos. According to Jason Benitez, deputy chief of the DSS Security Office, "Recently the DSS Security Office provided personnel with opening and closing procedures for individuals who are authorized to secure spaces within DSS facilities across the nation. In providing this training, the Security Office was able to utilize the CDSE's training video, which provided knowledge on the correct methods of operating combination locks and has assisted greatly in ensuring DSS personnel are trained appropriately."

COURSES USING VIDEO

The following courses each leverage videos to maximize learning:

EFFECTIVE COMMUNICATION IN DOD SECURITY

This graduate-level distance learning course incorporates 39 videos into instruction. The videos provide essential models of various communication styles, including topics such as body language, corporate storytelling, and engaging presentation techniques.

The videos imprint models into students' memories that would not be possible through other written delivery mediums.

THE DOD SECURITY SPECIALIST COURSE

This self-paced course is delivered through the CDSE Collaborative Learning Environment (CLE) and consists of 24 blocks of instruction in video format as well as eight "how to" videos.

Each of the content blocks is narrated by an instructor and provides foundational course information using a visually engaging style to pique students' interest, gain their attention, and foster increased content retention. The video format also lets students pause and replay the content, leading to better understanding and enhanced learning experience.

NATIONAL INDUSTRIAL SECURITY PROGRAM OVERSIGHT COURSE

Also delivered through the CDSE CLE, the NISPOC course uses videos that demonstrate both appropriate and inappropriate interview techniques and methods of communication.

The video format allows viewers to see the speaker's posture and facial expressions, as well as hear the corresponding speech tones and pacing in both face-to-face and telephonic communications. Students can identify with the video scenarios and are likely to remember them upon entering the field.

A Q&A with **Craig Kaucher**, Chief Information Officer

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

Craig Kaucher was selected as Chief Information Officer (CIO) in March 2015.

He is a Defense Intelligence Senior Leader and a retired U.S. Army officer. As the CIO, he is responsible for the technological infrastructure, key information technology support services, and day-to-day administration of technical government personnel plus support contractors in execution of the DSS mission.

Prior to joining DSS, Kaucher served as the first Chief Information and Technology Officer for the Defense Media Activity (DMA), where his focus areas and priorities were to improve the standardization and effectiveness of the technology architecture across DMA, improve and create more efficient technology acquisition practices, and to strengthen the information security posture of the organization.

He also served as the Director for Information Sharing and Knowledge Management, and CIO in the Office of Intelligence and Analysis, Department of Homeland Security. He was the founding government employee of this division and of the CIO function in this organization.

Kaucher's final military assignment, as a U.S. Army lieutenant colonel was as the professor of Information Operations in the Information Operations and Technology Department, Information Resources Management College, National Defense University, where he taught in the NSA/DHS certified Information Assurance certificate program, as well as in the DoD CIO certificate program, and the Advanced Management Program.

He began his military career as an Army Signal Corps officer and served in a variety of assignments from the tactical to the strategic level.

Tell us about your background? What led you to this position?

I have 32 years of federal service, as an active duty Army officer and federal civilian. All of that time has been in the national security area with about a third in the intelligence community. While I've always been in the information technology field, I have enjoyed being part of the day-to-day operations of the intelligence world. It's compelling work and for an IT person, very interesting.

I was drawn to DSS because of its mission. It does stand out as unique in the Department. It's a small agency with a national mission. The overall scope of the work was also interesting. I think there are a lot of technology challenges and opportunities here, and I wanted to work somewhere where I could be part of that IT challenge.

Since arriving at DSS, you've spent some time traveling to the various DSS locations. What was your goal with these visits and what have you learned?

My goal in visiting the various DSS locations was to understand, at a grassroots level, how we are doing from an IT perspective. I wanted to know what the average person in the field thought about the CIO at DSS. I talked directly to employees at all levels to get a deeper understanding of their mission; what they actually do?

And when I say 'field,' I did visit our field office personnel and that was a very big part, but I also talked to personnel in the headquarters office and the directorates. I wanted to capture the IT challenges of the internal workforce and see what the CIO can do to better support them.

I found that we, the CIO, are very strong in some areas, and woefully inadequate in others. I also found the agency is very dependent on the Microsoft Office suite of programs. For instance, Financial Management does much of their work with Excel spreadsheets and Access databases. They don't have an end-to-end system; we're really just using these tools to track activity. The new system DSS is building, the National Industrial Security System or NISS, is designed to sweep up a lot of those Office products, as well as some really antiquated databases.

CDSE [Center for Development of Security Excellence] is another example. They have a lot of ongoing initiatives and are a unique microcosm that has a huge impact; but also a huge challenge from the customer base they serve to stay current and relevant. So there are some really good things we're doing, but we're falling behind in other areas.

This is your third position as a Chief Information Officer. How is this position different from the others you have held?

This position is unique for me as I came into an existing CIO organization in a well-established agency. When I joined Homeland Security, the agency was less than a year old. The director was new, employees were just getting to know each other and there was no technology staff at all. I was building an organization from the ground up.

When I joined the Defense Media Activity (DMA), it had just been formed in response to a Base Realignment and Closure requirement. DMA was formed from service components and DoD, and it came with a small IT shop, but the elements were scattered and there was no CIO. So again, a new position.

In coming to DSS, I found a stable agency with an established staff. That's a very different situation to walk into. I found initiatives that were already ongoing, such as NISS and the DITMAC [DoD Insider Threat Management and Analysis Center]. I also found processes in place and we've adjusted some of those, but there was a lot of good thought and ideas from the CIO staff on what to do and how to perform.

I also immediately found support from across DSS, such as Security, Human Capital Management Office, etc. When I started at DHS, those offices weren't fully formed which made the job even more challenging. I've also been able to very quickly engage with the Financial Management and Acquisitions offices which are our most important internal partners in DSS. So I was able to immediately discuss issues with them and talk about how we could improve.

What do you see as the biggest challenge facing the OCIO?

I think the biggest challenge is changing priorities and keeping the workforce focused on those priorities. We also need the staff to articulate the priorities so we can understand them and adjust without something slipping through the cracks. A lot of our focus has been sharpened around the cyber security environment, but this causes a ripple effect. For instance, recent cyber events have caused us to rethink our stance on cloud computing. We're still looking at it, but we need to ensure we're doing the right thing the right way and are doing it well before we make the leap.

> "The greatest strength of the CIO is **the really sharp people who work here**. They are **some of the most talented I've seen** in government."

What do you see as the greatest strength of the CIO? And conversely, what most concerns you about the CIO?

The greatest strength of the CIO is the really sharp people who work here. They are some of the most talented I've seen in government. They think ahead and they are very good at coming up with ideas on how to improve. I have been very impressed with what they bring to the table.

My concern however, is with the size of the CIO staff relative to its workload. I worry about burning people out. Too much change can wear people down. So we have to be clear in our priorities and stay focused on them.

What is on the horizon for the CIO?

I see DSS looking at other ways to obtain shared technology services so we don't have to maintain the systems ourselves. And by that I mean services such as enterprise email and cloud computing.

We're already doing a lot of this. For instance, we don't run our own travel system or our own time and attendance system. Instead we leverage shared services and other service providers for these processes that we take for granted.

By doing this, the CIO can then focus on the core systems and processes that are unique to DSS, such as NISS or the ODAA Business Management System. So we will continue to look for opportunities to leverage these other systems.

DSS establishes Insider Threat Identification and Mitigation Program

Editor's Note: Due to high profile events such as the Washington Navy Yard shooting, WikiLeaks and Fort Hood shooting, insider threat has garnered renewed interest across the government. Based on new executive requirements, DSS has stood up an internal insider threat function, as well as one focused on supporting the personnel security investigations for industry mission.

The following two articles provide an update on those efforts. These two articles do not address the National Insider Threat Policy for cleared industry, as those requirements will be outlined in Conforming Change 2 of the National Industrial Security Program Operating Manual.

by Randy Laylo
Counterintelligence directorate

In November 2012, the White House issued the National Insider Threat Policy and Minimum Standards for executive branch insider threat programs. These standards provided DoD and its agencies with the minimum elements necessary to establish an effective insider threat program.

These elements include the designation of a senior official; capability to gather, integrate, and centrally analyze and respond to key threat-related information; monitor employee use of classified networks; provide the workforce with insider-threat awareness training; and protect the civil liberties and privacy of all personnel.

To meet these requirements, DSS established the Insider Threat Identification and Mitigation Program (ITIMP) in 2013 with the goal of deterring, detecting, and mitigating the insider threat, and thereby minimizing any potential damage an insider can have on national security.

This program integrates and leverages DSS expertise in security, counterintelligence, information assurance, antiterrorism/force protection, human capital management, and other relevant functions and potential information sources such as the inspector general and office of general counsel to identify and mitigate any perceived insider threat to DSS or its systems.

The ITIMP is an inward facing program that focuses on DSS government and contractor personnel, joint duty assigned personnel, and industry partners directly supporting DSS within assigned and controlled DSS space.

Through the ITIMP, DSS will work to deter, detect, and mitigate the insider threat.

An **insider** is defined as any person with authorized access to any U. S. government resource to include personnel, facilities, information, equipment, networks, or systems.

An insider threat can use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States.

This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

The Insider Threat: Industry Division

by Lovely Rodriguez and Andrew Woods
Counterintelligence directorate

Chi Mak admitted to being sent to the United States in 1978 by China to obtain employment in the defense industry with the goals of stealing U.S. defense secrets, which he did for 20 years. In 2007, he was convicted of conspiracy, failure to register as an agent of a foreign government and other violations.

Michael Mitchell, a disgruntled employee, was fired from his job due to poor performance. He kept computer files with his employer's trade secrets and entered in a consulting agreement with a South Korean company and gave them stolen trade secrets. In 2010, he was sentenced to 18 months in prison and was ordered to pay his former employer over $187,000.

Aaron Alexis, a cleared contactor, fatally shot 12 people and injured three others at the Washington Navy Yard in 2013. He had a pattern of criminal behavior and poor employee conduct. The shooting was the second deadliest mass murder on a U.S. military base, behind the Fort Hood shooting in November 2009.

What do these three cases have in common? They are all insider threat cases. Due to today's technological advances and increased use of removable media, insiders can now carry more information out the door in only a matter of minutes; information that can take years to collect. The motivation for these insiders varies from greed/money, allegiance to another country, to personal ego.

Unfortunately, the insiders that become a threat have far reaching consequences to both their organization and national security. According to recent FBI cyber investigations, businesses incur significant costs ranging from $5,000 to $3 million due to cyber incidents involving disgruntled or former employees. The damage to national security is immeasurable, and a threat to the sense of freedom we all enjoy.

To identify and detect insider threats within cleared industry, the Counterintelligence directorate, Insider Threat for Industry branch serves as a counterintelligence review team for the personnel security investigation mission for industry under DSS purview. The branch provides analysis when potential insider threat and/or counterespionage indicators are identified in an employee's personnel security investigation or other credible reports.

The branch provides analysis when **potential insider threat and/or counterespionage indicators** are identified in contractor's personnel security investigation or other credible reports.

To execute this mission, DSS relies on a cadre of counterintelligence agents who have a strong knowledge and expertise in personnel security and the insider threat program. The branch provides direct support to both DSS field and headquarters personnel and other federal government agencies, in addition to supporting the Department of Defense Consolidated Adjudication Facility (DoD CAF).

The team provides pertinent details to help inform the decision made by the DoD CAF to grant or deny an individual a personnel security clearance. If necessary and/or warranted, analysts also write reports for referral and/or potential investigative action by other federal law enforcement agencies.

The Insider Threat for Industry branch has made a significant contribution to identifying and detecting insider threats within cleared industry. These efforts have helped ensure the protection of classified information and controlled sensitive information in the hands of cleared industry.

DSS Inspector General Hotline

An Exercise in **Cooperation, Collaboration & Partnership**

by Gary Morgan
DSS Inspector General

The mission of the DSS Office of Inspector General is to provide the DSS Director fair and independent oversight of the DSS mission through impartial and independent inspections, assessments, investigations, inquiries, and teaching and training. The office is staffed by the DSS IG, the deputy IG for assistance and investigations and the deputy IG for readiness.

The DSS IG Hotline was established in fiscal year 2010 and is managed by the deputy IG for assistance and investigations.

The DSS Hotline provides a confidential and reliable vehicle for military service members, DoD civilians, cleared defense contractor employees, and the public to report fraud, waste, mismanagement, abuse of authority, and issues surrounding the security of classified information resident within our cleared industry partners.

The DSS Hotline received over 400 contacts in FY15; and nearly 48 percent of all DSS Hotline contacts deal with issues related to the National Industrial Security Program.

As an example of a NISP issue, in November 2014, a concerned cleared contractor employee contacted the DSS Hotline alleging that his company, holding a Top Secret facility clearance and safeguarding approved to the Secret level, had failed to adequately address a classified data spill identified by DSS during the company's last security vulnerability assessment (SVA) in 2013.

The DSS IG collaborated with the complainant to clarify the issues, coordinated with Industrial Security Field Operations, and notified the appropriate regional office of the potential security violation. After conducting an administrative inquiry at the facility, the field office determined that corrective actions had not been taken and the magnitude of the spill was considerably larger than initially reported.

The field office followed up with an SVA two weeks later and identified the possibility of 10 years' worth of contaminated back-up tapes stored in a non-NISP compliant environment in four uncleared facilities with numerous uncleared personnel involved. The facility received an unsatisfactory rating and an invalidation of its facility clearance.

DSS IG HOTLINE:
Toll Free: 1-888-865-1508
Commercial: (571) 305-6660
Email: inspector.general@dss.mil

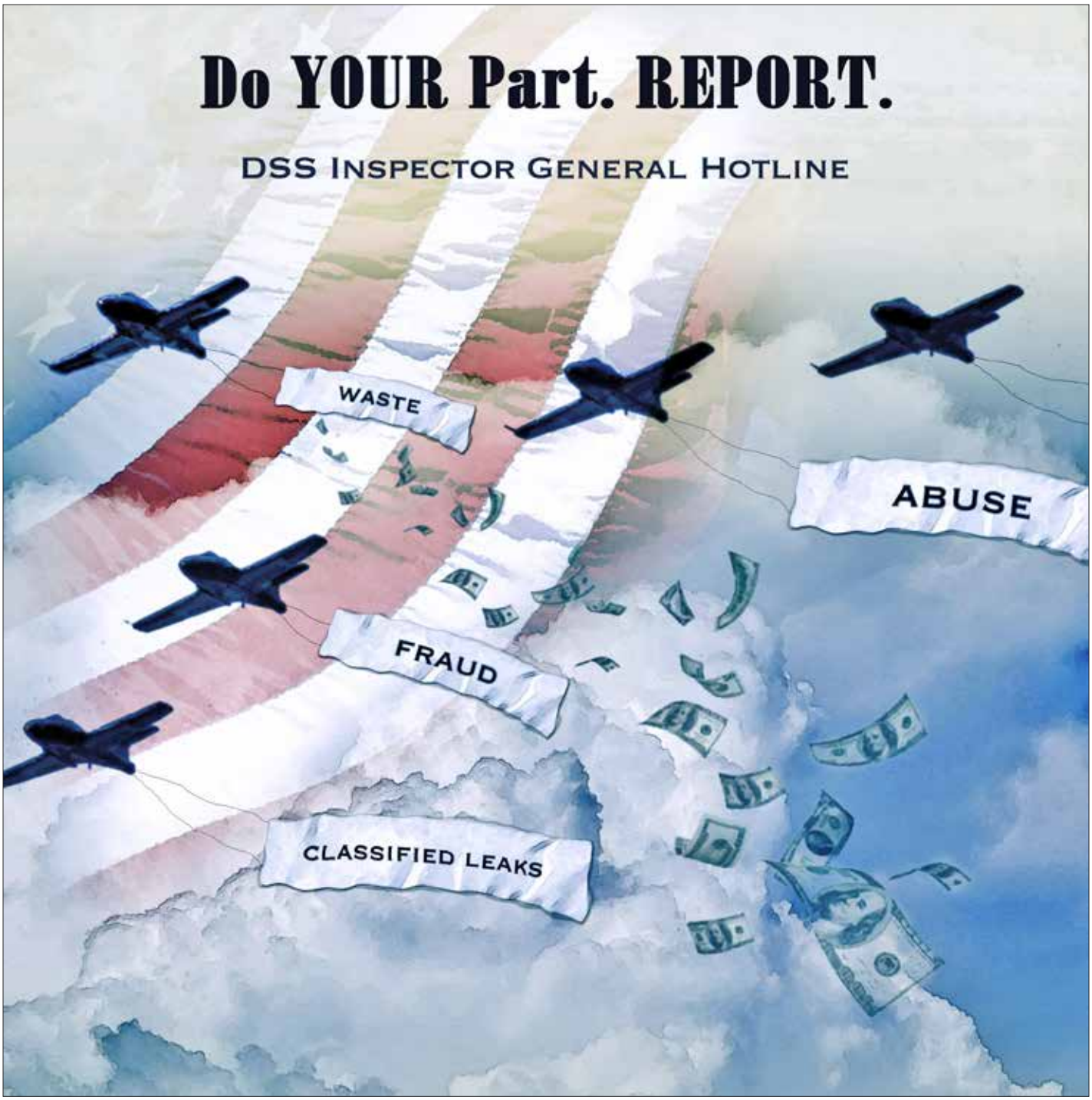
However, not all contacts on the DSS Hotline involve allegations of waste, fraud, abuse, and mismanagement. A significant number of clients are looking for answers to questions or have a problem that they either don't know how to resolve or are looking for guidance. This type of contact falls within the DSS IG's assistance function.

Over 100 DSS IG Hotline contacts, or roughly 25 percent of FY15 contacts, requested assistance with personnel security clearance (PSC) issues.

With the transfer of the oversight of the Joint Personnel Adjudication System to the Defense Manpower and Data Center (DMDC) in 2010, and the subsequent creation of the DoD Consolidated Adjudications Facility (DoD CAF), there is no central point of contact for public queries into the status of a PSC. Therefore, the DSS Hotline continues to receive requests for assistance and provides the public with accurate and timely information.

Resolving these issues requires collaboration with DMDC, DoD CAF, Office of Personnel Management, the Personnel Security Management Office for Industry, the International Division, and industry partners. While DSS IG doesn't have the ability to fix the client's clearance issues, it is able to provide information on the process and point them in the right direction toward resolving the issue.

In 2014 the DSS IG, assisted by DSS Counterintelligence directorate, briefed DoD Hotline personnel on topics of interest to DSS in its NISP oversight role. As a result of



this engagement, the number of DoD Hotline actions sent to the DSS IG increased 400 percent.

For instance, one of the inquiries, generated by an anonymous DoD IG Hotline complaint, resulted in the mitigation of a potential security violation and insider threat posed by a cleared employee at a cleared defense contractor. DSS IG coordinated with DSS field office personnel and another Defense agency to investigate the allegations. The employee was terminated and his/her access to classified information was revoked. The coordination and collaboration with other DoD agencies, DSS directorates, and industry partners mitigated a potential threat to both classified information and employees of a cleared defense contractor.

Through close coordination, cooperation and partnership with DSS employees, and government and industry stakeholders, the DoD IG is able to see significant benefits from the DSS IG Hotline.

e-QIP Click-to-Sign replaces manual signature process

by Zaakia Bailey
Personnel Security Management Office for Industry

As a part of the personnel security clearance process, an employee must complete an Electronic Questionnaire for Investigations Processing (e-QIP) and signature pages. The signature certification and release pages authorize the investigation service provider to obtain the necessary information.

In the past, these forms had been signed by the subject and sent to the facility security officer (FSO) via fax, mail or scanned and uploaded into the Joint Personnel Adjudication System (JPAS).

Missing or illegible signature pages account for approximately 95 percent of the cases the Office of Personnel Management (OPM) rejects each year. As a result, the manual signature process could significantly delay the processing of the e-QIP.

In today's fast paced environment, where transactions are processed as quickly as you can click a button, the use of **Click-to-Sign provides greater efficiency** in the personnel security clearance process.

In today's fast paced environment, where transactions are processed as quickly as you can click a button, the use of Click-to-Sign provides greater efficiency in the personnel security clearance process.

When the e-QIP is complete, the applicant simply clicks a box and proceeds to the next step, submitting the Standard Form 86 to the FSO and Personnel Security Management Office for Industry (PSMO-I).

In using Click-to-Sign, the applicant's user ID and password login capability remain the same, and no PKI certificates or special software is required. The applicant/FSO can still print and save a copy to include the release pages.

For initial investigation requests, there is no impact to fingerprint submission. OPM will schedule the investigation when the e-QIP, release pages and fingerprints are received.

While applicants can't be required to use Click-to-Sign for the release documents, it is strongly recommended. If a person decides not to use Click-to-Sign, the FSO will know when the applicant opts out.

However, the FSO will no longer be able to upload these documents into JPAS. Instead, the FSO will have 72 hours to provide manually signed pages to click2sign@dss.mil before the e-QIP is rejected.

The development of Click-to-Sign involved several agencies, to include the Defense Manpower Data Center and OPM, who worked aggressively to modify JPAS and e-QIP in order to enable Click-to-Sign and optimize user experience.

Additionally the U.S. Army G-2 and the Department of Energy were instrumental during the testing and implementation phase with OPM.

Click-to-Sign uses the appropriate safeguards to ensure that the digital signature captured in the e-QIP system is legally recognized in accordance with the Federal Electronic Signatures in Global and National Commerce Act 15 U.S.C. 7001 and the Uniform Electronic Transaction Act. Public Law 105-277, Title XVII states "Releases that are digitally signed are as valid as those with handwritten signatures."

Knowing the difference between a professional certification program and a certificate program

by Stephanie Fox
Center for Development of Security Excellence

The Security Professional Education Development (SPēD) Certification Program is a professional certification program that assesses the knowledge, skills, and competencies a security professional acquired through their experience and training. But how is this different than a certificate program?

According to the Institute for Credentialing Excellence, an assessment-based certificate program is a non-degree-granting program that awards a certificate only to those who have taken a specific course of instruction and passed an associated examination measuring whether the participant met the course's learning outcomes.

While specific training is required for an assessment-based certificate program, maintaining that certificate is not. For instance, once someone earns a CPR certificate from the American Red Cross, the certificate is good for two years. The participant need not do anything. That is, there is no requirement for any continuing education during those two years.

By contrast, a professional certification program delivers an assessment based on security community knowledge, is independent from training courses, and grants a time-limited credential to anyone who meets the assessment standards.

A certification program mandates continuing education credits within a specified span of time to keep a certification active. Active certificants in the SPēD Certification Program must attain 100 professional development units within their two-year maintenance cycle to maintain and renew their SPēD certifications.

SPēD certification carries with it a credential individuals may use once they are conferred. For instance, John Smith, conferred the Security Fundamentals Professional Certification (SFPC), may refer to himself on business cards and other documentation as "John Smith, SFPC" while his certification is active.

The SPēD Certification Program has received national accreditation by the National Commission for Certifying Agencies for three of its certifications: SFPC, Security Asset Protection Professional Certification, and Security Program Integration Professional Certification.

To learn more about the SPēD Certification Program, please visit http://www.cdse.edu/certification.

Professional Certification Program

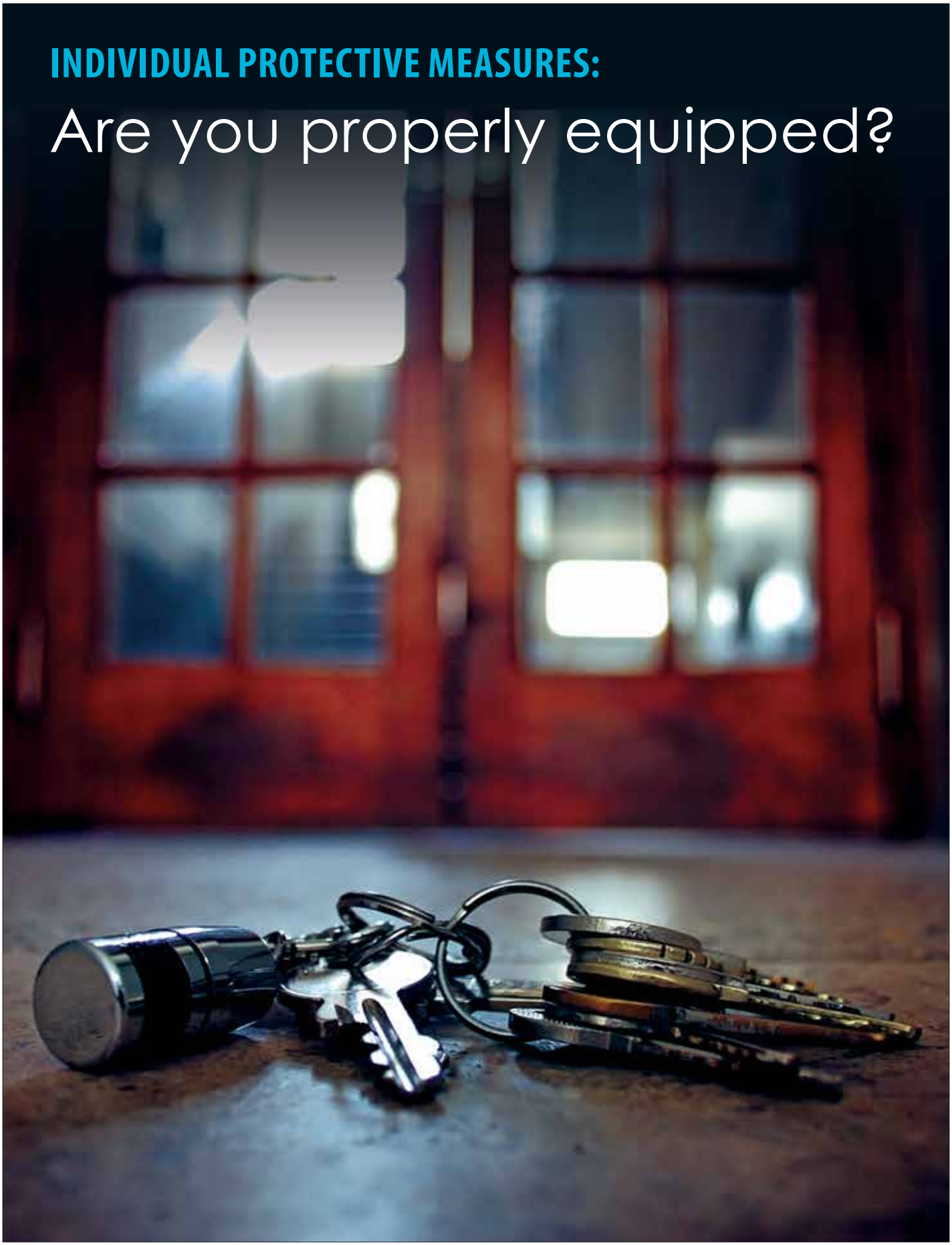
- Assesses previously-acquired knowledge, skills, and/or competencies
- **Goal:** To validate the participant's competency through a conforming assessment system
- Assessment is used to assure baseline competencies and differentiate professionals; independent of a specific learning event
- Assessment content is typically broad in scope
- Awards designations to recognize achievement

Assessment-Based Certificate Program

- Provides instruction and training
- **Goal:** For participants to acquire specific knowledge, skills, or competencies
- Assessment is used to evaluate mastery of the intended learning outcomes; linked directly to the learning event
- Assessment content may be narrow in scope
- Awards a certificate to recognize mastery of specific learning outcomes

INDIVIDUAL PROTECTIVE MEASURES:

Are you properly equipped?



by Ken Beckett
DSS Antiterrorism Officer

While most of us aspire to live a good life, one only needs to watch the news to know that at any given time, potential threats could disrupt our lives with violent or destructive acts.

With a little planning, you'll be better prepared to detect, react, and respond to dangerous incidents and potential threats.

Here are some general security tips:

- Memorize key phone numbers (home, family, office, security/emergency services, etc.), so you'll have them handy in an emergency
- Don't publicly identify yourself as being affiliated with the federal government. Stay away from civil disturbances and demonstrations.
- Be unpredictable in your movements. Vary your daily routine, to include your route to and from work, and the time you leave and return home.
- Don't give out information regarding family travel plans. If going to an unfamiliar locale, know the nearest location of emergency services, such as police, fire stations, and hospitals.
- Do not give personal information over the telephone and avoid giving personal details to anyone unless their identity can be verified.

HOME TIPS

- Keep track of keys to your home and if a key is lost or stolen, change the locks.
- Do not open your home to strangers or people you cannot positively identify. Check the identity of unexpected workers with property management before allowing entry.
- Keep your doors (including the garage entry) locked at all times, especially at night, even if you are home!
- Do not store junked vehicles and structures on your property. These make good hiding/observation sites for bad guys.

SECURITY PRECAUTIONS WHEN YOU'RE AWAY

- Leave the house with a lived-in look. Use a timer to turn lights and TV/radios on and off at varying times and locations throughout the house. Secure your valuables and ask a trusted friend or neighbor to check your home periodically.
- Stop deliveries of newspapers and mail. Mail can also be held at the post office.
- Do not advertise your plans on social media, email or telephone voicemail.
- Do not hide keys outside the house. Leave keys with trusted neighbors or co-workers if necessary.

VEHICLE SECURITY

- Always look around and inside your vehicle before entering to check for anything suspicious or out of place.
- Consider the following steps to prevent potential vehicle tampering.
    - Always secure the doors and windows of your vehicle.
    - Become familiar with the mechanical and electronic tamper-prevention systems and devices on your vehicle.* Locate the hood release latch within the driver's side of the cabin, and ensure that it functions properly.
    - Vehicles with latch release fuel access covers and locking fuel caps provide additional anti-tamper features to possibly discourage potential threats.
    - Install an intrusion alarm.

  * If your vehicle is not equipped with these features, consider having them installed or activated.
- If you find something out of the ordinary, DO NOT TOUCH THE VEHICLE! Immediately move to a safe location, preferably where you can continue to observe the vehicle, and contact law enforcement authorities.

Becoming Proficient with Your Tools

Employing these tools regularly will help you be better prepared for any potential threats. Actions that are effectively and efficiently repeated over time eventually become easier to perform, even under duress. Want proof? Look at how easy it is for you to tie your shoe laces, even when your attention is directed in other areas!

Be alert, be aware, and be safe out there.

"HEAR YE, HEAR YE!": Employees of the Capital Region listen to Heather Green, regional director, at the all hands recently.

Integration, recognizing insider threat discussed during Capital Region all-hands training

by Doug Stone
Regional Operations Manager, Capital Region

Integration within the region was the focus of the Capital Region's semi-annual all-hands training, held recently at the Center for Development of Security Excellence, Linthicum, Md. Approximately 100 industrial security representatives, information systems security professionals, counterintelligence special agents, and regional leaders participated.

The goal of the workshop was to enhance integration by formalizing horizontal and vertical collaboration and coordination, as well as engagement opportunities among the region and other DSS directorates. The desired outcome would be unified decision making in support of the agency mission. The DSS Office of Innovation (DOI) led the workshop and discussion.

The agenda featured 10 breakout groups that brainstormed to identify which field actions were currently integrated and which actions were not. Each group then determined what steps needed to be taken in the Capital Region to reach full integration and who was responsible for making this integration happen.

Additionally, a topic of discussion during the workshop was identifying the insider threat within an organization. Guest speaker Sandy Grimes, former Central Intelligence Agency officer, led a discussion on the book, "Circle of Treason — A CIA Account of Traitor Aldrich Ames and the Men He Betrayed."

Grimes, a veteran of the Clandestine Service, recounted how she participated on a small team that investigated and uncovered the actions of Aldrich Ames, a CIA officer who was subsequently convicted of spying for the Soviet Union.

Grimes' portrayal of events that took place during her time as a CIA officer piqued the audience's interest resulting in a lengthy question and answer session.

Stan Sims, then DSS director, provided a DSS update, held a question and answer session with regional personnel, and awarded several DSS director coins for performance excellence.

ANDOVER, MASS.

Field office open house fosters partnership, communication

More than 200 cleared contractor security professionals recently attended the Andover Field Office open house in Andover, Mass.

The contractors who attended represented 120 companies within the Andover area of responsibility, including New Hampshire, Maine and six counties in Massachusetts. Personnel from the Northern Region office also participated in the event.

The goal of the annual event is to foster a partnership with industry by allowing both DSS employees and industry attendees to get better acquainted with one another, the Andover facility and the assessment environment.

The event also introduces industry security professionals to the entire field office and region staff and showcases the field office's upgraded capabilities.

The highlight of the event, according to many attendees, was participation from then DSS Director Stan Sims, who addressed the audience and answered several questions.

Feedback from industry included the following remarks *(continued on page 26)*:

GATHER 'ROUND: Attendees of the Andover Field Office open house listen to then DSS Director Stan Sims (center).

"

Thank you for having us! It was a great event, and meeting the director was pretty significant for us Facility Security Officers who would probably never get the chance otherwise. **I particularly appreciated that the DSS reps were willing to talk shop with us** although that was not exactly the purpose of the open house. I think the open house was a success. Don't change anything!

Fantastic event. Great to see everyone in their own environment and **great to get input on what it is like on a day-to-day basis at the field office**. I felt privileged to be able to hear Mr. Sims speak and was especially glad to hear his message about our partnership and his views on that. Positive experience all the way around.

"

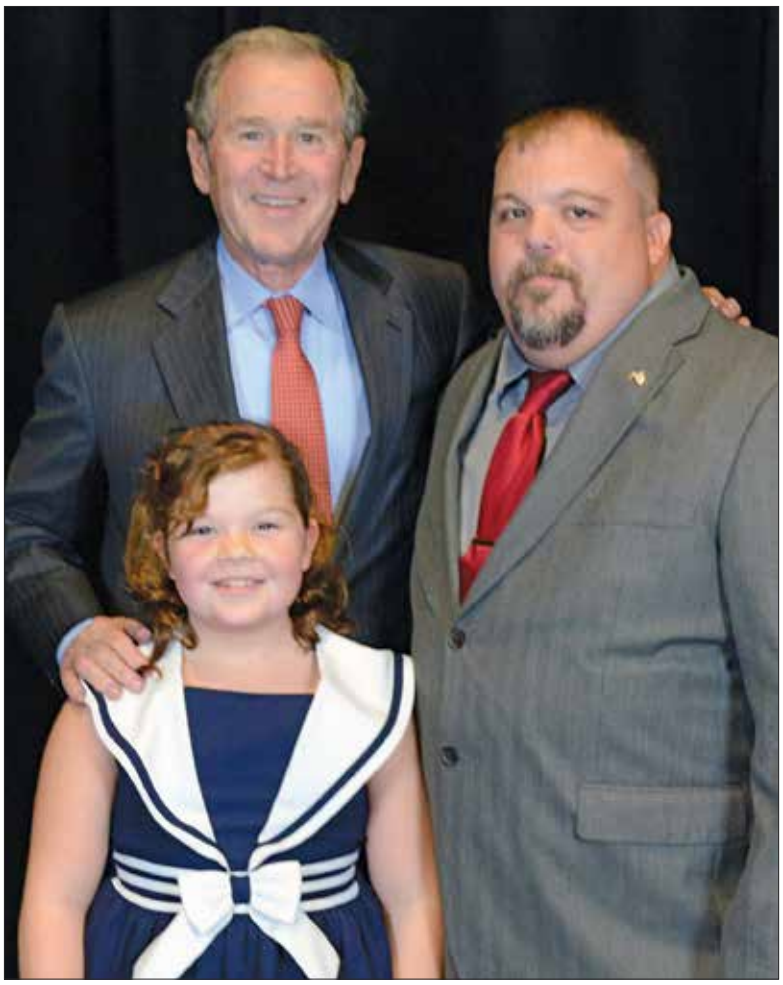
“

Thanks to your whole team for hosting us at your Open House last week. **DSS continues to perform as an active partner with private industry**. We need your continued support to combat the continuing threat of hackers on the network and insider threats.

Fantastic event — **so great to catch up with all the folks from DSS** that we interact with regularly in one setting (and not an assessment! :-). A great introduction to DSS for my FSO-in-training too!

First, I would like to thank you and your office for putting this event together and inviting us to attend. We enjoyed the opportunity to visit the Andover Field Office and meet with other representatives from other contractors as well as with the staff of DSS. **It was also a pleasure to meet with Director Sims**; I am glad that he was able to attend.

”



DSS EMPLOYEE MEETS FORMER PRESIDENT:

When John Myers, information systems security professional in the Irving Field Office, was getting ready to retire from the United States Navy in August 2015, he was looking for a guest speaker for his ceremony.

Among the emails he sent, one went to the office of former President George W. Bush. Myers received an immediate response indicating the president apologized and thanked him for his service, but would have to decline due to a prior commitment.

Myers responded that he understood, and maybe they could meet in the future for a chat.

Fast forward to November 2015, when Myers received an email invitation to an event where Bush would be the guest speaker. Myers and his daughter Ariel were treated like VIPs, seated in the front row, and were first in line to get their photo taken with the president after the event was over.

“President Bush was very humble, nice and awesome,” Myers said. “He thanked me for my service, asked Ariel how old she was, what grade she was in, where she lived and told her he was glad she was there. It was truly an amazing night, and Ariel and I are blessed and thankful to have had this rare opportunity.”

HAPPY BIRTHDAY TO YOU!: DSS Marines present at the ceremony (from left to right) were retired Staff Sgt. Michael Mylan, information systems security professional; retired Staff Sgt. Nazim Arda, counterintelligence special agent (CISA); retired Gunnery Sgt. Ryan Rivera, CISA; and retired Chief Warrant Officer 3 Michael Farley, regional designated approval authority.

Alexandria Field Office celebrates the Marine Corps' 240th Birthday

by Andrea Cole
Alexandria Field Office

On Nov. 10, 2015, the Alexandria Field Office celebrated the 240th birthday of the United States Marine Corps with a ceremony featuring retired Marines assigned to the agency. The Continental Congress established the Marines on Nov. 10, 1775, which has since been recognized as the U.S. Marine Corp's birthday.

Retired Gunnery Sgt. Ryan Rivera, counterintelligence special agent (CISA), orchestrated the ceremony, which included the reading of the 13th U.S. Marine Corps commandant's birthday message, a video of this year's birthday message, and the cake cutting ceremony.

The first piece of birthday cake is traditionally presented to the guest of honor, which in this instance Rivera said included all those present.

The second piece of cake was presented to the oldest Marine in attendance, who in turn handed it to the youngest Marine in attendance, symbolizing the experienced Marines passing their knowledge to the new generation of Marines.

DSS Marines present at the ceremony were retired Chief Warrant Officer 3 Michael Farley, regional designated approval authority; retired Staff Sgt. Michael Mylan, information systems security professional; and retired Staff Sergeant Nazim Arda, CISA.

Program unlocks **leadership potential** beyond the professional realm

Editor's Note: The below article is a personal account of two DSS employees' experience in the Federal Executive Board of Greater Los Angeles Leadership 2015 Associate Program.

by April Rodriguez-Plott, *Cypress Field Office*, **and Ehren Thompson,** *San Diego Field Office*

Leaders are not born, they are made. Leaders are shaped by experience, refined by challenges and developed through training.

In an effort to gain leadership training, two DSS employees participated in the Federal Executive Board (FEB) of Greater Los Angeles Leadership 2015 Associate Program. Initially the idea was to seek improvement and learn new skills to further develop our capacity as leaders.

Little did we know that the program would serve to unlock our potential beyond the professional realm. Participation in the leadership program required a self-conscious application of the lessons that resulted in an invigorated perspective of our value to DSS.

The FEB program was established by Presidential Directive in 1961 by President John F. Kennedy, to serve as a forum for communication and collaboration among federal agencies outside of Washington, D.C., since 85 percent of federal employees reside outside of the capital area.

This leadership program is designed to provide associates with intergovernmental experiences and interaction with federal executives in order to build a cadre of professionals with broad skills for the future.

The FEB leadership program is a one year commitment to training and seminar attendance in addition to selecting a mentor at the executive level of another federal agency. In addition, each participant completed a program project, and attended the required seminars and training sessions necessary to develop a leadership skills, such as leadership practices, networking, relating to others, time management and communication skills.

EHREN'S EXPERIENCE

My journey with FEB began in 2013. While working the Combined Federal Campaign for DSS, I met a gentleman who was an FEB fellow. As we spoke, he told me about the leadership associates program and the history of the FEB. I found the conversation interesting, but it was too late to apply for the next class. However, I kept the FEB program in mind for the next year.

One year later, I was accepted into the program, joined by my DSS colleague, April Rodriquez Plott, and we were the first DSS employees to attend the FEB Leadership Associates Program. At our first session, the program lead discussed course expectations, mentoring, curriculum, and other graduation requirements.

The key component of the program involved being mentored and collaborating with other federal agencies. More importantly, we were challenged to step outside our comfort zones and even our organizations as we began this journey. As leaders, we must be prepared to accept challenges and be uncomfortable.

May 19, 2015, the day I graduated from the Los Angeles FEB, was the culmination of a year of hard work, late days, long drives and lasting relationships. In the days leading up to graduation, I found myself reflecting on my personal involvement with FEB. I have been involved with leadership programs in past, but this course proved to be different in terms of commitment, time, expectations, and practicality.

Although a yearlong commitment seemed daunting at first, it passed so quickly that I almost did not notice. In the meantime, I have enjoyed a year of working with other federal employees and more importantly learning from these outstanding individuals.

APRIL'S EXPERIENCE

The FEB Leadership Program notably enhanced the quality of my professional and personal life. It helped me reshape my approach to organization, communication in and outside of the work place, but most importantly participation in the program affirmed my value — my value to our agency, my field office, to team members and contractors. Affirmed value grows confidence, generates vision and increases productivity.

In attending various training seminars and half day development series for the program there are many notable lessons to speak of but, here are the three most influential lessons that I now actively implement in daily approach to work. First, vision pulls us forward. Creating a daily checklist of priorities to execute for the day or week keeps me accountable, sharpens my focus and allows me to start each day with purpose and vision then

> Although a yearlong commitment seemed daunting at first, it passed so quickly that I almost did not notice. In the meantime, I have enjoyed a year of working with other federal employees and more importantly learning from these outstanding individuals.

TAKING THE LEAD: April Rodriguez-Plott (left), Cypress Field Office, and Ehren Thompson, San Diego Field Office, at the graduation for the Federal Executive Board (FEB) of Greater Los Angeles Leadership 2015 Associate Program.

end it with a sense of accomplishment. This approach to daily tasking allows me to align my workload with Industrial Security Field Operations priorities and stay on track.

Secondly, in daily interactions I seek to understand. When listening to others, I not only seek to understand what they're saying but I strive to understand the message that is sent about what they value. In response others feel valued and the doors for finding solutions and collaboration open up.

Lastly, push gratitude toward someone; a contractor, a colleague, the person assisting from the Defense Manpower Data Center help desk. Taking a few moments to reach out, thank someone or validate a job well done within our network only serves to strengthen relationships.

One of the greater lessons this program embedded in my understanding is that leadership has everything to do with relationships. When we joined the leadership program, we became a part of a greater network. In this network we learned about various federal agencies through executive interviews, selection of mentors at the executive level and the interagency participation was an incredibly fruitful networking environment.

We gained a greater understanding of the many facets of business sectors in the U.S. government. We felt especially proud to tell the DSS story. Pushing gratitude is vital to keeping us connected as we continue doing the critical work that keeps the warfighter safe.

CONCLUSION: OUR PLACE IN THE DSS VISION

Leadership does not always equate title, position or power. Daily, we can and should ask ourselves, "How am I improving the existing system as a leader, an aspiring one, or as a team member?"

We all have the opportunity to progress our leadership capacity. That's what we'll continue to do with our new, refined set of leadership skills as we better support and contribute to the DSS mission.

FY15: DSS by the Numbers

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

255 **Education Course Completions**

8,001 **Personnel** registered for **webinars**

105,776 **PDUs** [Professional Development Units] **Earned**

86,267 **Visits** to **Security Shorts**

324,196 **Visits** to **Toolkits**

784,422 **Course Completions**

4,944 **Conferrals** in Security Professional Education Development Certification Program

COUNTERINTELLIGENCE

39,437 **Reports of suspicious contact** from industry

6,913 **Referrals to Law Enforcement/** Intelligence Community

1,020 **Investigations/operations opened** due to DSS referrals

7,292 **Intelligence Information Reports**

3,872 **Personnel** attending seven **Counterintelligence Webinar** events

OFFICE OF THE DESIGNATED APPROVING AUTHORITY

39 **NISP Command Cyber Readiness Inspections** containing 44 circuit reviews

3,596 System security plans **(SSPs) accepted and reviewed**

Common deficiencies in SSPs:

1. SSP incomplete or missing attachments
2. SSP not tailored to the system
3. Inaccurate or incomplete configuration diagram or system description
4. Sections in general procedures contradict protection profile
    a. Missing certifications from the Information Systems Security Manager
    b. Incorrect or missing ODAA Unique Identifier (UID) in plan/plan submission
    c. Missing variance waiver risk acknowledgement letter

2,587 Completed **system validation visits**

Common vulnerabilities found during system validations:

1. Security-relevant objects not protected
2. Auditing: Improper automated audit trail creation, protection, analysis, and/or record retention
3. SSP does not reflect how the system is configured
4. Inadequate configuration management
5. Topology not correctly reflected in (M)SSP

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:

PERSONNEL SECURITY MANAGEMENT OFFICE FOR INDUSTRY (PSMO-I)

940,000 National Industrial Security Program (NISP) **contractors with clearance eligibility**

860,000 NISP contractors with **access to classified information**

180,000 **Requests for investigation** for security clearances processed

80,000 Interim **security clearance determinations** made

8,000 **Adverse information reports** triaged

8,000 **Overdue** periodic investigations

300 Interim **clearance suspensions** in process

FOREIGN OWNERSHIP, CONTROL OR INFLUENCE (FOCI)

535 **FOCI facilities**

239 **Mitigation Action Plans** in place

18 **FOCI Action Plans** emplaced

INTERNATIONAL ACTIONS

3,047 **Requests** for **Visits**

11,554 **Travelers**/Visitors

823 **NATO Visit** Requests

1,640 **NATO Travelers**/Visitors

229 **Transportation** plans

215 **Hand Carry** Plans

30 **Security Vulnerability Assessments**

INDUSTRIAL SECURITY FIELD OPERATIONS

5,376 **Security Vulnerability Assessments** conducted *(including Excluded Parents)*

9,084 **Security Vulnerabilities** identified

8,339 **Non Acute/Critical Vulnerabilities** identified

745 **Acute/Critical Vulnerabilities** identified

1,168 **Facility Security Clearances** issued

Defense Security Service