DSS ACCESS

Official Magazine of the Defense Security Service | **Volume 7, Issue 1**

THIS ISSUE

Facilitated workshops next step in launch of leadership development program

DEFENSE SECURITY SERVICE | PARTNERING WITH INDUSTRY TO PROTECT NATIONAL SECURITY

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: FACILITATED WORKSHOPS NEXT STEP IN LAUNCH OF LEADERSHIP DEVELOPMENT PROGRAM

INSIDE

ASK THE LEADERSHIP

AROUND THE REGIONS

From the Director

By the time you read this issue, we will already be three months into 2018 and almost halfway through the fiscal year. Suffice it to say, it's been a challenging start to both, but DSS continues to lead the way in protecting the security of our nation and supporting the warfighter.

I held a town hall in early January for all DSS employees to articulate my priorities for the year. I want to reiterate a few of those priorities here. 2018 will be a year of transition for DSS. Over the past year and a half, the work we have done with industry to develop and refine the new methodology under DSS in Transition has established a solid foundation on which to build the next layer. Thanks to industry's involvement and feedback, which have been invaluable, we are ready to begin rolling out the new process in an incremental way that educates both DSS and industry as we continuously improve on it. This is a fundamental shift in how we oversee the National Industrial Security Program, but it's necessary. We can no longer continue to do business as usual; as our adversaries adjust, so must we.

DSS will begin to implement the phased transfer of the background investigation mission from the National Background Investigations Bureau to DSS in accordance with the FY18 National Defense Authorization Act. I know people are anxious about this transition and unsure what it means to their positions, DSS, and even DoD. We are very early in the transition process -- although we have notional timelines associated with the move, we will not take action until we're ready. There are too many details to rush headlong into this process. We will be deliberate and meticulous in our approach, with a goal of minimizing disruptions to the overall clearance process and also to DSS operations. We have a unique opportunity to fundamentally transform the vetting process and institute real and meaningful change. In this, we must not fail.

I also will continue to fight in 2018 for resources, including additional field positions and to facilitate the movement of our counterintelligence function into the Intelligence Community. I think this move will help the IC leverage DSS' unique expertise and access, while opening new educational and training paths for DSS personnel and enabling threat information sharing between and among IC agencies.

As you can see, we have a full plate and this just scratches the surface! I am confident that DSS will succeed in each of these areas and strengthen our ability to protect the nation's most critical assets and technologies.

Dan Payne
Director

Facilitated workshops next step in launch of LEADERSHIP DEVELOPMENT PROGRAM

by Larry Cunningham
Leadership Development Program

As part of the recent launch of the DSS Leadership Development Program (LDP), 74 DSS employees participated in three different Facilitated Leadership Development Workshops (FLDW) during August-October, 2017, at the Center for Development of Security Excellence (CDSE).

The FLDWs provided an introduction to leadership concepts and methods, as well as a forum for participants to demonstrate and apply what was learned through presentations, discussions, and practical exercises designed to encourage development of leadership skills, abilities and behaviors. Each session was conducted by cohort, which is defined as a group of individuals who share a particular event together during a specific time frame. Participants in the LDP will remain in their cohorts through the Leadership Conference in June 2018.

The DSS LDP is developing leaders across DSS, and its foundation is based on leadership development competencies required for two tiers of employees -- GG7-GG13 (Tier 1) and GG14-GG15 (Tier 2). Employees selected to participate in the LDP were required to complete two Skillport pre-requisite competency learning programs, and prior to attending the FLDWs, were required to complete several assessments to understand how they handle information, make decisions, and function within the structure of an organization. Additionally, co-workers and supervisors completed an online assessment about each participant.

At the kickoff of each cohort, students were divided into three or four teams. These groups were designed for collaboration during the FLDW, as well as communicating with each other for the duration of their time in the LDP.

DSS partnered with the Center for Creative Leadership (CCL) to develop and deliver the cohort-based LDP. The DSS LDP team and CCL representatives collaborated on the initial framework and delivery concept. The CCL facilitators delivered tier specific workshops with the following expectations for the participants:

Tier 1:

- Identify their own leadership strengths and weaknesses and have a plan to address them
- Recognize and choose more effective ways of

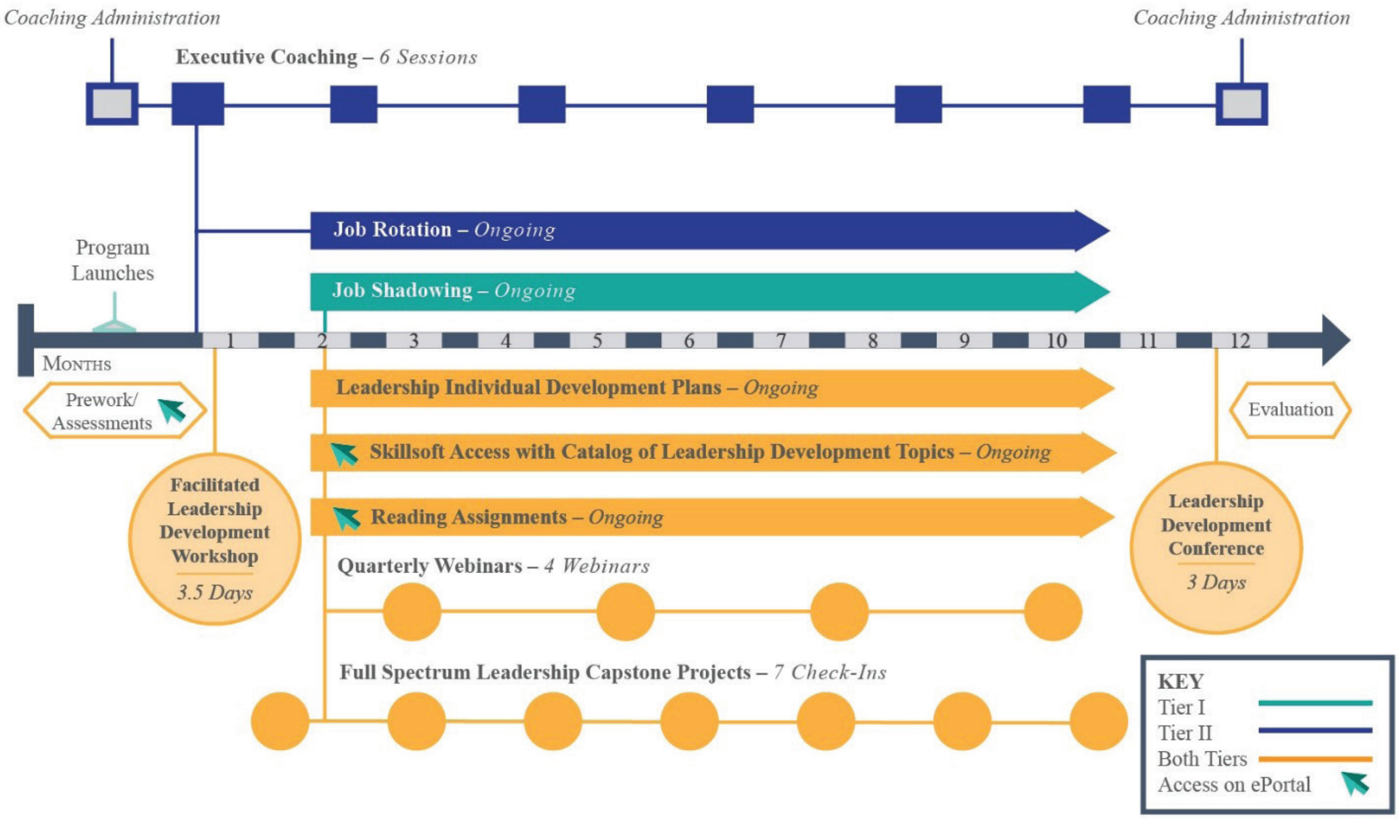
communicating with others
- Use influencing and conflict skills to strengthen relationships
- Use the Situation, Behavior, Impact (SBI) model to share constructive feedback
- Build sustainable relationships with peers and teams by understanding the unique needs and preferences of each team member
- Improve learning agility through critical thinking
- Identify and set goals to build a more effective leadership brand

Tier 2:
- Think and act strategically to effectively address DSS challenges
- Manage tactically with strategic impact
- Coach and lead others through complex and ambiguous tasks
- Lead others through conflict
- Lead others through organizational change
- Blend organizational change and transition with managing and running an operation

During the three cohorts, participants were assigned Capstone projects that are designed to address a specific DSS challenge or issue, and to synthesize all aspects of leadership learning using a team-based model. Working with their designated teams, the participants developed a solution and the results of these team projects will be presented to DSS senior leaders during the LDP Conference scheduled for June 19-22, 2018.

As a part of the DSS LDP, participants review materials or engage in assignments through the course of a year. These include:

1. Behavioral style assessments
2. Leadership 240- or 360-degree assessments
3. Use E-portal for LDP activities, resources, etc.
4. Catalog of leadership development topics
5. Quarterly webinars focused on leadership topics
6. Shadowing assignments for Tier 1 and rotation experiences for Tier 2
7. FLDWs
8. Full spectrum leadership capstone assignment
9. Reading assignment
10. Leader Individual Development Plan (IDP)
11. Executive coaching (Tier 2 only)
12. LDP conference
13. Keynote speaker during LDP conference


Coaching Administration
Coaching Administration
Executive Coaching – 6 Sessions
Program Launches
Job Rotation – Ongoing
Job Shadowing – Ongoing
1
2
3
4
5
6
7
8
9
10
11
12
Months
Prework/ Assessments
Leadership Individual Development Plans – Ongoing
Skillsoft Access with Catalog of Leadership Development Topics – Ongoing
Reading Assignments – Ongoing
Facilitated Leadership Development Workshop 3.5 Days
Quarterly Webinars – 4 Webinars
Full Spectrum Leadership Capstone Projects – 7 Check-Ins
Evaluation
Leadership Development Conference 3 Days
KEY
Tier I
Tier II
Both Tiers
Access on ePortal

In their own WORDS

A sampling of attendees were asked to provide feedback on their experience with the LDP and the FLDWs. Here are their thoughts in their own words.

Quinetta Budd

Communications Program Specialist
Office of Public and Legislative Affairs

"Before arriving for the facilitated workshops, everything was explained upfront and all of the attendees' questions were answered. I appreciated all the communication prior to the training, and completing the prep work beforehand saved a lot of time. At the training, the instructors had such great personalities and a way of including everyone in every activity. We utilized every minute of the training without feeling tired or overwhelmed. I learned that anyone can be an effective leader, whether they're an introvert or an extrovert. During the role playing activities, we discovered what was considered an appropriate response to different situations in the workplace; there isn't always a right or wrong way and sometimes you just have to take into account different personalities, situations, and backgrounds to get a positive result.

"The most important thing I learned during the workshop was about my likes/dislikes and comfort zone in a professional environment, based on my personality. Also, staying positive, learning as much as I can about my job, taking initiative, and training will help me achieve my leadership goals. Your personality, conduct, and daily interaction with others can help you as a leader. There are other people in the program who are similar to you so we are all learning together and from each other - it's not a competition. This program offers guidance on how to be the leader that you want to be."

Franklin Caul

Training Specialist
Human Capital Management Office

"The training pre-requisites focused on the introduction and development of leadership competencies identified within DoD, which helped prepare me for the facilitated workshops. I enjoyed the two day face-to-face sessions, which included a group session with a trained coach to encourage team building and planning. The peer learning groups provided quality feedback sessions, which provided insights into myself, as well as suggestions and support for professional growth.

"The hands-on exercises, including a business environment simulation, allowed for deeper learning. Topics focused on improved communication, setting and achieving goals, and developing decision making skills.

"Since becoming a part of the LDP, the skills I have learned have made an immediate impact on my career and my current projects. I would recommend anyone in DSS attend the LDP at any stage in your career."

Dessie Howard

Industrial Security Representative, Hanover Field Office
Industrial Security Field Operations

"The LDP experience thus far has been an invaluable experience. It has afforded me the opportunity to learn about myself while interacting with others. I think that the environment is designed to teach you how to interact as opposed to react during difficult conversation and situations. During the week of the onsite I learned that my strength in the workplace is building and maintaining relationships; but I need to work at communicating using the Situation, Behavior, Impact (SBI) model approach. I am utilizing the SBI approach to communicate professionally and personally. When giving feedback to individuals I find myself using words that express a positive impact more during conversations and I am trying hard to rid my thoughts of words that express a negative impact (overwhelmed was a word that I used quite often). I feel more comfortable using words like I need to hit the "Refresh Button" now! I believe the benefit of attending LDP is that it provides you with a platform on which to grow and be nurtured prior to being placed in a leadership position without the appropriate tools to succeed. I believe the LDP will produce confident, competent and enthused leaders."

Ashley Maddox
Chief, Contract Operations
Office of Acquisitions

"I have thoroughly enjoyed the program. The one week workshop was a great experience. It was nice to have an opportunity to work with and meet other individuals from different directorates. The workshop information and feedback taught me a lot about myself and allowed me to see myself differently than I had previously. The FIRO-B, Big 5 and 360 assessments provide a lot of detailed information that has been extremely beneficial for my growth. Being able to talk through those assessments and the results with my coach has provided even more insight for me to dig deeper. Through the assessments, I learned that my peers and direct reports see me to be a stronger leader than I thought I was. It has helped build my confidence in some areas, while still providing multiple areas of development and leadership growth. The feedback has been key and very valuable. I've already started applying the information that I've learned towards day-to-day duties. I have taken the feedback that was provided during the workshop, along with the information provided from my 360 assessments and started making changes to my daily operations with my direct reports, peers, customers and leadership. I am interested in getting into further detailed conversations with my coach about recommendations for my growth.

"The program really provides a lot of information that is beneficial. There is a lot of work that goes into the program - assessments, reading, individual training courses, the workshop, Capstone project, papers and is difficult to do with daily work requirements mixed in but if you're willing to put in the work, you will get so much out of this program. The specific benefits that I've seen are: an insight into myself, learning my strengths and weaknesses, learning how to take and work with constructive criticism, and expanding my contacts through the agency."

Areece Peak
Field Office Chief, Boston Field Office
Industrial Security Field Operations

"The Facilitated Leadership Development Workshop (FLDW) was comprised of a diverse group of high performers, and sessions were highly interactive to improve our leadership skills. I've learned to expand my self-awareness as a leader and take personal time to pause, listen, and reflect more. I also learned how I learn best, recognize my limits, and strive for quality and competence in all that I do. Classroom instructions and simulations meant a new understanding of being intentional in the way I lead my field office. I think at times we, as supervisors, get complacent and 'stuck in ruts' from time to time in leading others, and I recognize now that I needed some prompting to bring a freshness back to ensure I am leading effectively, efficiently, and with a purpose.

"Some of the topics covered during the workshop were important to truly identify our strengths and areas of improvements, in order to lead others, organizations, or departments to achieve success. The instructors were top-quality and group simulations were excellent. As always, sharing ideas and experiences with colleagues was beneficial, and the schedule allowed time for learning and reflection. I will absolutely utilize the techniques, lessons learned, and continuous feedback from colleagues to

> "...I needed some prompting to bring a freshness back to ensure I am **leading effectively, efficiently, and with a purpose**."

improve my leadership to create positive change through DSS in Transition (DiT). I have been very fortunate to participate in formal opportunities similar to this workshop to develop my leadership skills. The benefits of this workshop/program were different in that it focused on 'me' and my self-awareness, and that has given me a tremendous exposure to new opportunities to accelerate my growth as a leader."

Hollie Rawl
Visual Information Specialist
Center for Development of Security Excellence

"The LDP Facilitated Leadership Development Workshop really focused on the importance of understanding oneself; highlighting not only how personality and work/study preferences shape personal perceptions of the world, but, more importantly, how others might perceive those words and behaviors. Honing in on these innate personality preferences incredibly increases self-recognition of strengths and weakness, allowing the ability to not only pinpoint areas of improvement, but also the ability to use those strength areas as a powerful starting block to connect with, and inspire, others.

"As a previous graduate of the Office of Personnel Management LEAD Certification Program, I entered the DSS LDP program with higher expectations than most other participants. The DSS LDP is definitely meeting those expectations by focusing on the importance of developing a well-rounded individual with awareness tools and leadership skills that can transcend even the most challenging or stressful situations. By drawing on my OPM LEAD experience I am able to provide both positive and constructive feedback to the LDP leadership team in order to ensure DSS not only provides an excellent leadership training program, but further exceeds government precedent. With an agency-focused initiative to train leaders on all levels, the DSS program is off to an incredible start that will surely result in a strong leadership culture increasing mission readiness, improved employee relations, and high retention rates.

"Regardless of one's interest in a future supervisor or team lead position within their office, participation in DSS LDP would be beneficial. The program not only creates an atmosphere for in-depth reflection and acute self-awareness for personal improvement, stress management, and resiliency, it provides critical training on core interpersonal skills such as communication, conflict resolution, and team building. As if those aren't enough incentive to join the program, an additional highlight is the ability to not only partner with employees across the agency to tackle problems facing DSS from an employee-based standpoint, but to also formally present change management solutions to the DSS directorates for implementation. DSS has taken an impressive step towards increasing mission effectiveness through a personnel development approach and we should take full advantage."

> "Regardless of one's interest in a future supervisor or team lead position within their office, **participation in DSS LDP would be beneficial**."

Nicole Rhodes,
Space Management Specialist
Logistics Management Division

"The LDP is a 12-month developmental program focused on deepening the DSS leadership 'bench.' I had the privilege of attending the inaugural workshop kicking off the program. The workshop started with an overview of the program -- 12 months, two workshops, four webinars, seven check-ins, 100 book recommendations, one leadership shadowing, and a Capstone project, after which we delved into four days of self-discovery. The program prerequisites focused on individual assessments that included a 360 evaluation and several behavior-based assessment surveys. The results of the survey tools were presented, interpreted and applied throughout the workshop. The information each of us learned about ourselves and how we are perceived by others created the foundation of the program. After identifying your individual strengths, challenges, and preferences you can begin to shape how you want to be perceived by others. I consider myself to be rather 'self-aware' but for me, the value in the program is to show you how others view you, as well as, the impact your behavior has on other people and situations - for good or bad.

"The workshop set up the way ahead for the remainder of the program, which include periodic webinars, check-ins with the facilitator advisors as well as other cohort members. Training is routine for many DSS staff, as it's easy to attend a training, return to the office, and go back to business as usual. I found the outreach/check-in activities continually bring focus back to the program principles, keeping me engaged in the learning activities. The program is more involved than I anticipated but I am looking forward to working through the various learning components and working with my Capstone team. I would recommend this program to anyone in DSS that is interested in learning about themselves and shaping DSS into the future."

> ...the **value in the program** is to show you how others view you, as well as the impact your behavior has on other people and situations.

Rojohn Soriano
Curriculum Manager, Industrial Security (Internal)
Center for Development of Security Excellence

"As a result of the LDP, I've had the opportunity to meet and work with many people from across DSS, and it's interesting to note that we share the same goals and challenges in our daily work as leaders no matter where we work in the agency. The workshop in October was a great experience, where my cohort started to learn more about ourselves as leaders and will continue to do so throughout the program. I discovered quite a bit about myself, both on professional and personal levels, and that what goes on in one area directly affects another area. I've learned how my peers and superiors view me as a leader through the various self- and 360-degree assessments we've completed within the program. These assessments provided valuable insight, and goals for me to accomplish as I further develop as a leader within the program and well after I complete it. I've already started applying some of what I've learned in the short time I've been in the DSS LDP. One of the goals I identified for myself as a leader is to be more comfortable in making decisions in high pressure or time sensitive situations with less than complete data or information. That's obviously something many people encounter on a regular basis. I've faced several such situations recently and began applying what I've learned in my interactions with the LDP coaches/instructors, as well as during my individual coaching sessions.

"I think some of the benefits of the program include developing well-rounded and sound leaders who will be better prepared to lead others not only in DSS but throughout the government. I think the program benefits BOTH new leaders and those with previous leadership experience in the military, industry, etc. The DSS LDP provides an opportunity for participants to reflect and gain new leadership skills or adjust their leadership style to be more effective in the environment they are now working in. A colleague mentioned that when he first came to DSS, he had recently retired from the military and had to quickly learn that some of the things he did as a leader in the military were not necessarily effective in his new position. I also know colleagues who had wished they had a similar program such as the DSS LDP when they first became a supervisor. So I think the DSS LDP goes a long way in benefiting new and experienced leaders, as well as the people under their charge."

> I think some of the benefits of the program include developing **well-rounded and sound leaders** who will be better **prepared to lead others** not only in DSS but throughout the government.

Director lays out agenda at town hall

DSS Director Dan Payne laid out his priorities for the agency in 2018 during a town hall held in early January. In his opening remarks, Payne cited the National Security Strategy approved by the administration in 2017. It outlines four pillars:

- *Protect the American People, the Homeland and the American way of life.*
- *Promote American Prosperity*
- *Preserve Peace through Strength*
- *Advance American Influence*

"In reading the National Security Strategy," Payne said, "I was both surprised and proud of the number of times I saw the role of DSS in the strategy, and highly recommend that everyone read it and think about the role DSS plays in protecting our country."

Payne then quoted several portions of the strategy that were particularly relevant to DSS:

"Every year, competitors such as China steal U.S. intellectual property valued at hundreds of billions of dollars. Stealing proprietary technology and early stage ideas allows competitors to unfairly tap into innovation of free societies."

"We must prevent the theft of sensitive or proprietary information and maintain supply chain integrity. The U.S. must increase our understanding of economic policy priorities of our adversaries and improve our ability to detect and defeat their attempts to commit economic espionage."

"Our task is to ensure that American military superiority endures, and in combination with other elements of national power, is ready to protect Americans against sophisticated challenges to national security."

"This is the exact message I have been conveying for the past couple of years," said Payne. "This is the reason we need to alter our methodology."

Payne also cited the FY18 National Defense Authorization Act (NDAA), which has at least 17 sections that deal with security, many of which directly relate to DSS. "The necessity of protecting our critical technology is recognized at the highest levels of the U.S. government," Payne continued. "As stated, the protection of our critical technology is vital to the security and survival of this nation...and DSS plays a critical role in that mission. Each and every one of you play a critical role in that mission. The relevance and importance of what DSS does grows every day."

DSS Director Dan Payne briefs on the status of the DSS in Transition initiative during the agency town hall.

Payne then moved into specific changes coming to DSS. He said DSS had spent 2017 researching, planning and thinking about a new methodology. In 2018, DSS will begin to implement it. He described a phased approach that will begin with an initial trained field cadre who will focus on four facilities with critical technology. The goal is to concentrate on one technology and develop tailored security plans that can then be expanded. Payne said he expects the field to touch most of the facilities in their area of responsibility during the year, but not as a full vulnerability assessment.

Payne then discussed the language in the FY18 NDAA which directs the transfer of the background investigation mission from the National Background Investigations Bureau (NBIB) to DSS. He reiterated the phased transfer plan DSS had delivered to Congress and that the goal was to design a better process incorporating continuous vetting. "We want to help reduce the burden of the investigation," said Payne, "but we also have to maintain the highest level of security."

The remaining priorities Payne addressed concern additional billets and resources, moving the Counterintelligence directorate into the Intelligence Community and delivering JWICS to the field.

Following his formal remarks, Payne then spent the remainder of the time fielding questions from across the agency. Most questions addressed specifics of the new assessment methodology and how the field could be better integrated to implement it. "I don't have all the answers right now," said Payne. "But we will continue to learn as we implement and adjust as we need to. Our current processes are not effective and we have to change. I know it won't be easy, but we are moving to a vastly improved process that will better serve national security."

Payne also addressed possible reorganizations with the new NBIB mission, but said it was too soon to make any decisions. He did say DSS had started the process of looking at geographic overlaps where DSS and NBIB locations were collocated, or more importantly cities where one had a presence, but the other didn't to leverage resources. He also noted the new office space secured in Falls Church to support the landing team that will help facilitate the transition. "Ultimately," he said, "we would be looking at a facility in the Fort Meade area to consolidate the Continuous Evaluation team, the PSMO-I [Personnel Security Management Office for Industry] and CDSE [Center for Development of Security Excellence] under one roof with close proximity to the DoD CAF [Consolidated Adjudications Facility.]"

Payne also recounted the kick-off meeting DSS held with NBIB to introduce subject matter experts who can begin to engage on the myriad details associated with the transfer. "This will be a long process and we are just getting started," he said.

The rest of the questions focused on the results of the most recent Defense Equal Opportunity and Management Institute (DEOMI) survey and Federal Employee Viewpoint Survey (FEVS), and how leadership was addressing employee concerns. Payne said DSS would not conduct another DEOMI survey this year and had initiated a number of conversations concerning the most recent FEVS results. "We are taking an enterprise approach and addressing a number of changes, from a revised hiring guide to focused training to updated EEO policies."

TOP: Carey Williams, Diversity and Equal Opportunity Office, captures a comment by the director at the DSS town hall. **BOTTOM:** DSS senior staff listen, take notes on the topics covered at the DSS town hall.

DSS senior leader named as Presidential Rank Award winner for 2017

La Shawn Kelley

La Shawn Kelley, a Defense Intelligence Senior Level (DISL) and chief of the Human Capital Management Office (HCMO), was named a Meritorious Senior Career Employee for 2017.

The Civil Service Reform Act of 1978 established the Presidential Rank Awards Program to recognize a select group of career members of the Senior Executive Service (SES) for exceptional performance over an extended period of time. Later, the Rank Award statute was amended to extend eligibility to senior career employees with a sustained record of exceptional professional, technical, and/or scientific achievement recognized on a national or international level. Two categories of Presidential Rank Award are available:

- Distinguished Rank recipients are recognized for sustained extraordinary accomplishment, and only one percent of the career SES or senior level may receive this rank.
- Meritorious Rank recipients are recognized for sustained accomplishment, and no more than five percent of career SES or senior level members may receive this award.

In announcing the award, Kelley was recognized for the following accomplishments:

- Developed and implemented the Director Awards Program, which recognizes employees who have demonstrated the highest standards of excellence and dedication in support of the agency's mission. The Director Awards Program is designed not only to publicly recognize superior employee performance and innovation, recognition is also tied to how their efforts demonstrate the agency's core values, promoting a culture of positive reinforcement that becomes self-sustaining.

- Established the DoD Operation Warfighter (OWF) program at DSS to identify temporary internship assignments for service members convalescing at U.S. military medical centers. She leveraged the support of DSS senior leaders and collaborated with Defense Intelligence Agency OWF coordinators to build a model program that could be implemented at DSS headquarters, as well as in field offices across the nation. To date, DSS has hosted 54 OWF interns in a wide range of disciplines and has received accolades from members across the Intelligence Community (IC) for growing and advancing this valuable program.

- Led a forward-looking and strategic initiative to develop competency-based career maps for mission and support occupations. As DSS evolved to address the complexities of the national security mission, this initiative focused on the professional development of its most valuable asset…its people. DSS career maps are based on competency frameworks from DoD and the Intelligence Community, and provide comprehensive career paths for advancing within and across occupations within DSS. Career maps are broadly used across the agency as an ongoing mechanism to help employees enhance their skills and knowledge, which facilitates mastery of their current jobs, promotes career advancement, and initiates career planning discussion between supervisors and their subordinates. To date, 90 percent of all DSS employees have access to career maps specific to their occupations, which is important to creating an agile, technically competent, and professional workforce.

- Led the design and delivery of the DSS Leadership Development Program (LDP), an entirely new and innovative solution for leadership development within DSS. The LDP incorporates a foundational leadership culture based on DSS principles, core competencies, and mission objectives, and is designed to address progressive and continued leadership development needs of GG-7 through GG-15 employees over the course of their careers. Kelley's efforts ensured the LDP instituted a program that will be integrated into every facet of the employee life-cycle. The return on investment this program provides will continue to yield a sustainable and superior workforce of the future.

- Developed the agency's Strategic Human Capital Plan (SHCP), which aligns to the workforce objectives outlined in the DSS Strategic Plan 2020 and sets forth the direction for specific workforce priorities. Based on the SHCP, DSS is reviewing its hiring policies, conducting routine workforce assessments, using targeted recruitment to reach under-represented populations, and refining retention strategies to retain top talent.

- Recognized the value of diverse perspectives in the workplace and saw the Intelligence Community Joint Duty Assignment (JDA) Program as an opportunity to increase awareness of JDA opportunities within the Russell-Knox Building (RKB) at Quantico, as well as across the IC. Kelley partnered with agencies at RKB — the Naval Criminal Investigative Service, Army Criminal Investigation Command, Air Force Office of Special Investigations, and Defense Intelligence Agency — as well as the Defense Threat Reduction Agency, Marine Corps Intelligence Activity, National Geospatial-Intelligence Agency, and the Federal Bureau of Investigation, to plan and host the first JDA Information Exchange at RKB. Through her efforts, Federal employees across the IC were educated on how JDAs support career and professional development, and special emphasis was placed on RKB employees to highlight opportunities requiring no change in duty location or commuting pattern – creating a positive and mutually advantageous outcome.

A Q&A with **Heather Green**, Director, Personnel Security Management Office for Industry

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

Heather C. Green is the director of the Personnel Security Management Office for Industry (PSMO-I). The PSMO-I monitors personnel security eligibility and access for contractor personnel in the National Industrial Security Program; processes industry personnel security investigation requests; determines interim personnel security clearance eligibility for access to classified information; and provides incident report oversight, triage, and serves as a liaison between industry and the DoD Consolidated Adjudications Facility.

She began her career with DSS in 1997 as a special agent conducting background investigations prior to moving into the industrial security field. From 2002 to 2011, she was the chief of the Maryland Field Office where her responsibilities included management oversight of all aspects of the office, which included leading a team of industrial security specialists and providing security oversight to over 600 cleared contractor facilities. She has also served as the quality assurance manager for Industrial Security Field Operations (IO) where her responsibilities included the oversight of quality, consistency and standardization within IO. She became the director of the Capital Region in January 2013, and moved to PSMO-I in January 2016.

Q: Tell us about your background.

I started my career in DSS 20 years ago, as a special agent conducting background investigations. Shortly after, I transitioned to industrial security as an industrial security specialist, then Field Office Chief in the Maryland field office, Director of the Industrial Operations Quality Assurance Office and then, Director, Capital Region. In this position, I led the implementation of the National Industrial Security Program (NISP) by overseeing approximately 5,500 facilities with varying complexities and a diverse workforce of over 100 personnel (industrial security professionals and information systems security professionals) throughout seven field offices and ultimately ensured effective oversight over all aspects of the NISP.

In January 2016, I transitioned into the role as the Director of PSMO-I. This office consists of an amazing group of personnel security specialists focused on multiple functions to provide comprehensive end-to-end personnel security oversight of the NISP cleared population.

Q: What led you to this position?

Throughout my career, I have promoted a mission-driven culture that emphasizes the timely identification and mitigation of unacceptable risk. Understanding that personnel security is a critical discipline and ultimately the foundation to a solid security program, I jumped at the opportunity to lead PSMO-I. This is an exciting time in the era of personnel security reform and having the opportunity to help prepare PSMO-I for the future is extremely rewarding. My vision has been to instill a multi-disciplined approach to our jobs by fully integrating industrial, information and personnel security, and counterintelligence and I think we're well on our way to achieving this.

Q: Tell us about the mission of PSMO-I? What should readers know about the office?

PSMO-I is a centralized entity within DoD which manages the lifecycle of cleared personnel under the NISP, focused on risk. PSMO-I's responsibilities include the following NISP national security business activities:

- Executing the Personnel Security Investigations for Industry (PSI-I) budget to include validating need prior to submitting investigation requests to the investigative service provider.
- Making trust determinations for interim access to classified information and processing interim suspension actions.
- Overseeing industry cleared population and facilitating the early detection and prevention of insider threats by triaging incident reports, and processing requests for information (RFI) and investigations via non-standard periodicity.
- Integrating with DSS field offices by providing data and trend analysis and ensuring accountability of industry personnel security clearance maintenance.
- Conducting industry and government stakeholder outreach and engagement.
- Providing strategic planning efforts for community personnel security initiatives.

Q: The personnel security investigative mission has endured some budgetary challenges the past few years and PSMO-I has had to be creative in managing the workload. Is PSMO-I still facing these challenges?

Ensuring trusted individuals are able to perform on classified programs in a timely manner is a number one priority for PSMO-I.

DSS, on behalf of the Department of Defense and 32 Federal agencies who participate in the NISP, funds background investigations for contractor personnel security clearances. Currently, by interagency agreement, the National Background Investigations Bureau (NBIB) schedules and invoices investigations for the NISP on a cost-reimbursable basis.

Fiscal years 2016 and 2017 proved to be extremely challenging as DSS had significant PSI-I budget shortfalls. The budget shortfalls required DSS to meter submitting investigation requests to NBIB to stay within budgetary authority. This metering caused a significant delay in processing contractor personnel security clearances and had an impact on interim determination timelines. PSMO-I worked tirelessly to ensure we prioritized submissions and minimized the impact on mission critical programs.

The good news is that we are adequately funded for FY18 and have been able to significantly improve our timelines to include meeting our goal of 30-day interim determination reviews.

Q: Recently the Continuous Evaluation (CE) for the DoD Enterprise transferred to DSS. What is the status of that effort?

In December 2016, the DoD CE operational mission was transferred from the Under Secretary of Defense for Intelligence to DSS and PSMO-I. The PSMO-I CE division manages risk across the DoD eligible population by enabling earlier issue detection than traditional periodic reinvestigations. It also provides critical information to DoD component insider threat hubs by leveraging a set of automated record checks and business rules to assist in the ongoing assessment of an individual's continued eligibility. The CE division receives and triages alerts from the currently enrolled DoD population of over 1.1 million personnel (military, civilian, and contractor).

The CE division is driving requirements for a robust future state end-to-end CE process and engages with multiple internal and external stakeholders. The refinement and expansion of CE will ultimately improve risk management and investigative quality, reduce the cost of investigations, improve processing timelines, and lessen reliance on traditional reinvestigations, thereby mitigating increasing investigation prices, delays and backlogs.

Q: How will the passage of the FY18 National Defense Authorization Act which directs the transfer of the background investigative mission affect PSMO-I?

The transfer of the background investigation mission to DSS will certainly have an impact on PSMO-I. Since PSMO-I is the only personnel security operational element within DSS, we are providing significant contributions to the stand-up of the DSS background investigation mission. Our personnel are providing subject matter expertise to ensure a smooth, phased transition. CE will play a large role in phase 1 of the transition and the ultimate reform of the investigation mission. Through our focus on managing the lifecycle of cleared personnel, PSMO-I will continue to drive change to the personnel security mission to ensure only trusted individuals are allowed access to our nation’s most critical information and the potential insider threat is detected and mitigated.

DSS IN TRANSITION

Industry Core Group assists in risk-based asset identification for new methodology

by DSS Change Management Office

In 2017, the DSS launched an enterprise-wide change initiative called, "DSS in Transition." The goal of DSS in Transition is to move the agency from National Industrial Security Program Operating Manual compliance to an intelligence-led, asset-focused, and threat-driven approach to industrial security oversight.

Central to this initiative, DSS developed, refined, and is now testing a new methodology based on identifying the assets at each facility, establishing tailored security plans, and applying appropriate countermeasures based on the threat. Early on in the development of this new methodology, a number of partnership opportunities with industry became clear.

To transform these opportunities into action, DSS coordinated with the National Industrial Security Program Policy Advisory Committee and assembled a core group of 18 volunteers from cleared industry. The Industry Core Group first met in April 2017, and their collective thoughts, comments, and suggestions have helped inform and refine the development of the DSS methodology.

From the Industry Core Group's initial meetings, the members established a solid understanding of the DSS methodology. They learned that DSS is still going to conduct its core functions, such as performing security vulnerability assessments, providing advice and assistance, and responding to security events. Similarly, they also learned that the agency is changing the focus of its core functions from strictly evaluating facility compliance to protection of assets. As a result, the Industry Core Group recognized the critical importance of asset identification in the DSS methodology.

At the August 2017 Industry Core Group meeting, the members shared best practices on identifying assets; and were then introduced to tools, guides, and a framework developed by DSS to help cleared industry identify assets. At this meeting, DSS also asked for volunteers to participate in an Asset Identification Test.

From the Industry Core Group, five members volunteered to participate in the test. The test began in September and ended in late October 2017. The objective of the test was to: 1) evaluate resources DSS provided; 2) document processes actually used; 3) capture specific information on assets identified; and 4) share lessons learned.

For the test, DSS provided a security baseline template to capture asset identification information and proposed security controls, as well as providing "PIEFAO-S" asset category examples and a "cause-and-effect" fishbone diagram. PIEFAO-S stands for "People, Information, Equipment, Facilities, Activities and Operations, and Suppliers," and this tool identified a checklist of asset categories to consider. Similarly, a diagram was offered as a potential framework for critically thinking about and identifying assets.

In support of the test, DSS scheduled weekly conference calls to exchange information and introduce additional resources. Midway through the test, the calls were opened to the associated DSS industrial security representatives (ISRs), which provided ISRs with an opportunity to hear firsthand the full range of issues associated with developing an asset identification process.

From the initial test with the Industry Core Group, it became clear that for the DSS methodology to succeed, identifying assets will need to become a fundamental, ongoing, and evolving process in every cleared contractor's security program. Given this, the Industry Core Group volunteers have since continued their asset identification efforts and DSS has continued the conference calls on a bi-monthly basis. Looking ahead, the goal is to establish a steady and ongoing rhythm of testing, evaluating, and sharing best practices on asset identification.

Gortler receives senior level promotion

Fred W. Gortler III, director of Industrial Security Integration and Application, was promoted to the Defense Intelligence Senior Executive Service on October 1, 2017. In the above photo, Gortler is seen briefing at the 21st annual Foreign Ownership, Control or Influence (FOCI) Conference in July 2017. He joined DSS in May 2015 as a Defense Intelligence Senior Leader and has focused on transitioning DSS to a data-driven, partner-enabled and risk-based enterprise. Prior to DSS, Gortler commanded the Air Force 70th Intelligence Wing, was appointed to the Senior National Intelligence Service and served as director of National Intelligence Liaison with the Under Secretary of Defense for Intelligence, and was the Senior Mission Advisor for the National Ground Intelligence Center.

CDSE develops unauthorized disclosure training to meet White House directive

Cleared individuals have an obligation to protect classified information. Failure to do so can result in damage to national security and the warfighter. Reinforcing the need and obligation to protect classified information in an age of information sharing has presented a serious challenge to the federal government.

In July 2017, the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) informed DSS that the White House and the National Security Advisor would be releasing a memorandum focusing on unauthorized disclosure (UD) training for the federal workforce. In anticipation of this memorandum, the DSS Center for Development of Security Excellence (CDSE) developed a UD Toolkit.

The purpose of the toolkit is to help cleared individuals understand their duties and obligations, learn the difference between UD and legitimate whistleblowing, and determine where and how to report both UD and questionable government behavior and activities. It includes the following resources:

- Training (UD eLearning courses, job aids, webinars, and videos)
- Policies (national, DoD, and whistleblower)
- Awareness materials (case studies, posters, and prepublication review)
- Reporting (option to report UD activity and questionable government activity)
- Incident response (guidance for the general workforce, security personnel and other authorities)
- Additional resources

In September 2017, the White House directive was released, and outlined specific requirements for all federal executive agencies to meet in support of UD training and awareness. The memorandum specifically identified two CDSE eLearning training courses as meeting the training requirements.

Additionally, CDSE collaborated with OUSD(I) on a training format and deployment options that would support more than four million DoD and potentially other federal executive agency training users. To support the large influx of users, CDSE converted the identified UD courses to a video format accessible via CDSE's existing YouTube platform.

CDSE leveraged the toolkit, course, videos, and other resources to provide the training needed to help educate the federal workforce on unauthorized disclosure. The statistics show the impact to the security community -- the course videos reached a combined total of over 145,000 security personnel since their launch, the toolkit had over 120,000 hits, and the two eLearning courses exceeded 257,000 completions in FY17 and FY18. This use of technology and wide dissemination ensured that the training and resources needed to protect national security and help prevent future unauthorized disclosure would be available to anyone, anywhere, at any time.

DSS in Transition focus of annual supervisors training

by Robert L. Bivins
Industrial Security Field Operations

As illustrated in the farewell message in an Industrial Security Letter from over 20 years ago, the Defense Security Service (DSS) has been moving toward a risk-based approach to industrial security oversight for many years. Over the next year, DSS will finally begin implementing a risk-based approach developed from the DSS in Transition effort.

INDUSTRIAL SECURITY LETTER 97-1
Farewell message from Greg Gwash, deputy director for Operations, Defense Investigative Service; July 1997.

"For me, highlights have included the reinvention of the Industrial Security Program from a compliance-based activity to a service oriented, threat based program, and we brought counterintelligence expertise into DIS. Now we have the capability to recognize and neutralize many of the foreign intelligence threats to our sensitive information and systems, while implementing cost effective security counter-measures to reduce vulnerabilities. No longer do we impose blanket security requirements 'because the book says so.' It's called 'risk management'!"

During November 2017, over 100 supervisors from Industrial Security Field Operations (IO), Industrial Security Integration and Application, and Counterintelligence attended the annual IO Supervisors' Training at the Russell-Knox Building. The primary focus of the training was to prepare for implementing the DSS in Transition risk-based approach beginning January 2018. Over the course of three days, the supervisors received detailed, hands-on training on how to prioritize facilities for oversight and the way forward on a variety of DSS in Transition-related activities. Additionally, a practical exercise was done to incorporate hands-on experience in prioritizing facilities for oversight. Gus Greene, IO director, also provided an overview of the range of activities that IO will be conducting during fiscal year 2018 in implementing DSS in Transition.

Other key elements covered during the training included information on executing a range of oversight activities, to include end-to-end security reviews resulting in tailored security plans, and a variety of industry engagement activities designed to provide a sense of the security posture at a facility.

In addition to the training, the supervisors also received briefings from a variety of senior leaders, as well as the keynote speaker, Benjamin Richardson, deputy director for Information and Industrial Base Protection, Counterintelligence and Security, Office of the Under Secretary of Defense for Intelligence. Richardson opened the training with insight into department's efforts to protect national security from a high level perspective. This insight helped to highlight the important role that DSS plays in combatting the loss of technology.

Heather Green, Personnel Security Management Office for Industry (PSMO-I), director, provides an update on the activities at PSMO-I.

LEFT: Kyla Power, Industrial Security Field Operations, answers questions during the briefing on the redesigned security vulnerability assessment report. **RIGHT:** Gus Greene, director of Industrial Security Field Operations, briefs the status of the directorate's effort regarding DSS in Transition.

During his remarks, DSS Director Dan Payne was emphatic about his resolve to do what it takes to get the job done. In providing his insights on where DSS is heading and a recap of where DSS has been, he reiterated, "I took the job at DSS to help protect and stem the loss of critical technology." He said, "Training is essential to the new process. We want to roll out a fast moving, phased process." He also expressed his strong desire to push more decision making to the field and to support those decisions as long as employees are exercising good judgment to protect national security.

The supervisors received refresher training on handling and protecting classified information, along with briefings on the deployment of JWICS (Joint Worldwide Intelligence Communications System) to the field effort.

On the final day of training, Mike Buckley, Counterintelligence directorate chief of staff, briefed the supervisors on the actions being taken to bring the personnel security investigative mission back to DSS. Heather Green provided an update on Personnel Security Management Office for Industry and the initiatives the office has taken to reduce the timelines for interim eligibility determinations. Ray Campbell, director of the DSS Diversity and Equal Opportunity Office, closed the training with a session on the Defense Equal Opportunity Management Institute survey results and a second session on how to communicate better by connecting better. Attendees indicated they wanted more of this kind of training in the future, as well as additional training for personnel in the field on how to deal with all aspects of hostile or uncomfortable workplace environments.

The event showed attendees that DSS is prepared to implement risk-based oversight beginning in early 2018. After 20 years, DSS will finally achieve what Greg Gwash talked about in his farewell message in July 1997.

Sharpening critical thinking skills leads to better decision-making

by David Bauer
Director, Western Region

Editor's Note: *The following reflects the thoughts and opinions of the author on the importance of critical thinking in the decision-making process.*

Recently, discussion has centered on decision making and sharpening critical thinking skills to focus on those security and counterintelligence factors that put national security at an unacceptable risk. To be successful, we must understand what is important, what risk is, and what a proportionate response to risk is.

The *Foundation for Critical Thinking* defines critical thinking as the intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from, or generated by, observation, experience, reflection, reasoning, or communication, as a guide to belief and action. Critical thinking helps us make hard decisions, defend our positions, and helps us identify other solutions we might not have considered. Simply put, critical thinking is the ability to understand what is happening and consider all the data that will lead to better decision-making.

The DSS mission statement "through partnership and innovation, safeguard our Nation's interests as the premier provider of industrial security risk management and security professional development services" emphasizes the need to keep our eyes on the goal of the National Industrial Security Program (NISP), and not just the procedures of the NISP. We cannot expect a policy published in 2006 to keep up with the speed of change in technology and threats. For this reason, critical thinking is essential to our ability to identify and respond to the potential loss of sensitive and critical technology that will "safeguard our Nation's interests."

I suggest the more pressing question for DSS and our stakeholders is how is sensitive and classified information at risk and what can we do to eliminate or mitigate the risk? In the hypothetical scenarios presented below, which vulnerabilities place sensitive and classified national defense information at risk of loss? The answer to all these questions — "it depends." In the case of scenario 1, if an industrial security representative determined the Secret closed area was accessed by personnel working on a specific program and all cleared to Top Secret, would the risk of loss be greater or lower? In scenario 2, if a counterintelligence special agent determined cleared employees assumed everyone in the office space was cleared, left containers open and engaged in classified conversations with co-workers routinely around the workspace, would the risk of loss be greater or lower? In scenario 3, if an ISSP determined through interviews cleared employees had a high state of security awareness, would the risk of loss be greater or lower? In scenario 4, if the local facility security officer believed the corporate central clearance process is responsible for loading data into JPAS but committed to correcting it at their facility? In each of these scenarios, whether subject to correction under the National Industrial Security Program Operating Manual (NISPOM), the hazards each of these situations

Scenario 1:
Top Secret document discovered in a closed area approved for SECRET storage

Scenario 2:
Several cleared and uncleared employees intermingled in an area dedicated to a classified project, with multiple security containers and secure voice units

Scenario 3:
FSO is unable to provide records showing completed mandatory security education training of cleared employees

Scenario 4:
A centrally managed clearance management system fails to ensure incident reports are loaded into JPAS for adjudication

present requires DSS to think beyond the NISPOM to protect national security.

These are recent illustrations of vulnerabilities that require a deeper understanding of what is happening to identify the cause of the vulnerability and take appropriate action to reduce the risk to classified and sensitive information. In order to change the relationship between DSS, government customers, and cleared industry, we must be able to articulate why it is important to address a vulnerability, regardless of its relationship to the NISP. We are in a partnership, and within the partnership, we must be honest with each other on critical matters that will place national security decisions in the hands of national security decision makers.

So consider:

- Allow our mission to guide your actions: Recently, DSS Director Dan Payne stated that he expects DSS field personnel and leaders to use good judgment and be guided by our national security mission. Our leadership expects us to stand for the public interests and not avoid difficult discussions with cleared industry on the protection of national security (not solely on the nuances of NISP compliance). Even if our position does not win the day, our leadership and entire organization benefit from elevating the discussion of whether we (industry, government customers, and DSS) are truly meeting the spirit of the DSS mission.

- Be curious and question basic assumptions: Over the past two years, DSS has invested time and money into training a workforce that is curious. The days of an industrial security representative leaving a facility believing classified data was at risk, yet feeling they were required to give a satisfactory rating are over. For example, if a cleared company has a displaced workforce in a foreign country but has no suspicious contact reporting, we should not accept the lack of reporting because that is contrary to what we know is traditionally a threat vector exploited by foreign adversaries. Or, as in the case with scenario 2, even when we are told there are no inadvertent disclosures in an intermingled work force, common sense and experience tells DSS a disclosure and compromise of information will happen. Simply put, ask questions, trust your instincts, and express your concerns through conversations with cleared industry, your colleagues and field office chiefs, and remain focused on the evidence of protection versus the appearance of protection.

- Be aware of your bias and tendencies: Many years ago before leaving on vacation, I told my son, "No parties, take out the trash, and mow the lawn." When I returned, the lawn had not been mowed but a trash can full of beer bottles was at the end of the driveway two days before the scheduled trash pick-up. My son essentially did not do anything I asked. Three years later, I headed out on vacation, leaving my daughter home alone. I return to find the potted plants destroyed and immediately question her about having a party, which she denied. I was convinced otherwise based on similar experience three years earlier. Two days later, I saw a deer had climbed the balcony steps and was lifting the plants out of their pots. This is an illustration of how bias can influence our thinking. All of us have biases, but being aware of them and seeking to not draw the same conclusions from similar information without asking the right questions is what makes critical thinking possible.

- We are surrounded by experts: DSS may be the first, best, and only chance to identify and fix a vulnerability before it causes damage to national security. DSS is uniquely positioned because of our access to classified threat reporting and oversight of cleared industry to lead the discussion on the necessary countermeasures to protect sensitive and classified information within cleared industry. You may believe your situation or experience is unique, but chances are there are many DSS representatives that have encountered the same or very similar challenges. There's no reason to start solving a problem when someone has already laid the groundwork for the solution.

A DSS employee must strive to understand what needs to be fixed. Going back to the scenarios, each one represents some level of risk and shows that corrective actions are needed, but each requires further investigation to determine the root cause and appropriate tool to resolve the vulnerability with greatest effect. Once we become skilled at the art of curiosity and discernment, we will confidently stand before industry and our leaders and clearly explain the risk to our most important technology and defend our corrective measures.

Open houses fosters collaborative environment, partnerships

by Jennifer Morin
Boston Field Office

The Boston Field Office recently hosted open houses for cleared industry security professionals at its field office and at the Groton Resident Office in Connecticut. This is the second year of conducting open houses, and these events were attended by more than 80 security professionals, representing 70 companies from Connecticut, Rhode Island and Massachusetts.

These events foster a collaborative environment with local security professionals and senior management officials. DSS representatives discussed various topics, to include DSS in Transition, Risk Management Framework, insider threat program initiatives and counterintelligence updates. Field office personnel further engaged industry during a question and answer session which included the Northern Region Director Cheryl Matthew and Northern Region Authorizing Official Jeffrey Blood. There was significant participation from all in attendance, which promoted lively and relevant group discussions.

During the event, Matthew congratulated and presented Nancy O'Neil, Raytheon Company Senior Security Manager, with a DSS coin on her recent retirement announcement. O'Neil, who was recognized for her more than 30 years of industrial security experience, thanked DSS for the support provided to her throughout the years.

This year's events were a great success for the Boston Field Office, as they serve as an example of the continued importance of building and maintaining positive relationships with facilities participating in the National Industrial Security Program.

During the open house, Cheryl Matthew (left), DSS Northern Region director, and Areece Peak (right), field office chief, DSS Boston Field Office, congratulate Nancy O'Neil, Raytheon Company senior security manager, on her retirement.

Office integration takes time, requires mutual respect, understanding of mission

by Raymond W. DuVall
Tacoma Resident Office

Editor's Note: *The following is a firsthand account of how the Tacoma Resident Office has successfully integrated the counterintelligence, industrial security and information systems disciplines into a cohesive unit.*

How does a 1901 Friedrich Wanderer painting depicting various Renaissance artists have relevance to the DSS mission? Its owner, a counterintelligence special agent (CISA), states the painting is a representation of various skills coming together to improve the community – a prime example of integration.

Each person in the painting represents the top performer in that skill, with a group consciousness, shared vision, sense of purpose, and clear interaction. The painting is a visual reminder that the individual disciplines within the office can form into one integrated group. However, an interpretation of a painting does not always translate to real life. So how can we overcome the partition of responsibilities which creates the gulf between the DSS strategy and its processes, systems, and people?

Like all good efforts, there must be a shared vision which is directed in policy. In February 1993, the DSS Counterintelligence (CI) Directorate was established to foster the integration of CI into the agency's operations, in order to enhance security awareness and educate cleared industry about effective threat identification and reporting. Initially, it fell to each field office CISA to integrate CI through operational support, training, and policy development with industrial security representatives (ISR) and information systems security professionals (ISSP). Within the context of this vision, guiding our efforts were cultural transformation and increased awareness among disciplines about the value and relevance of the vision.

In this context, personnel in the office took the initiative to educate each other on their respective discipline requirements and what was needed for all disciplines to achieve mission success. This core group of senior people began coordinating all office actions across work streams, ensuring cross functional dependencies were resolved, reporting success results to executive leadership, and requesting resource needs to achieve further integration. This level of integration was not achieved overnight, but rather evolved through constant conversation between disciplines over a number of years and is still continuing.

Given time and stability, the next step in the process was to choose between staying with the current stove-pipe disciplines, which could inevitably lead to inefficiency, increased costs and present higher risks to the organization, or create an interdisciplinary culture that bridges disciplines to solve risk problems and aligns around the decisions that need to be made. First, office personnel need to see integration as a complement to core disciplines and not as competition. The office team needed to learn, respect and understand the roles of other team members which require personnel to accept criticism and act on it. To achieve this level of interaction the office team built informal relationships through camaraderie, fun and friendships in order to gain trust, mutual respect, reliability, commitment and support. Quite often, office personnel would go to lunch, which encouraged open discussion and an opportunity to get to know each other. The office also joined in social gatherings during sporting events on the weekend. Eventually, office personnel began to feel comfortable with each other and effectively interact on team project meetings thereby improving office procedures. Every office procedure and new program is now discussed and worked jointly by all disciplines. This has led to favorable comments by the region chief on the work of the office.

It's easy to underestimate the complexity and level of effort it takes to drive integration. True office integration requires people to combine their perspectives and expertise, and tailor them to the industrial security community so that the office product is more than the sum of the participating disciplines' knowledge. To achieve this, DSS Headquarters can act as a creative catalyst that identifies opportunities and provides a hub for integration policies, initiatives and methods. Individual field offices can then develop people who can provide leadership in creating an institutional culture where integration work is valued and facilitated.

FY17: DSS by the Numbers

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

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

168	**Education Course Completions**
50,949	**Personnel** registered for **webinars**
214,679	**PDUs** [Professional Development Units] **Earned**
94,295	**Visits** to **Security Shorts**
539,063	**Visits** to **Toolkits**
1,351,543	**Course Completions**
1,396	**Conferrals** in Security Professional Education Development Certification Program

INDUSTRIAL SECURITY FIELD OPERATIONS

3,839	**Security Vulnerability Assessments** conducted *(including Excluded Parents)*
6,458	**Security Vulnerabilities** identified
5,881	**Non Acute/Critical Vulnerabilities** identified
577	**Acute/Critical Vulnerabilities** identified
962	**Facility Security Clearances** issued

PERSONNEL SECURITY MANAGEMENT OFFICE FOR INDUSTRY (PSMO-I)

814,000	National Industrial Security Program (NISP) **contractors with clearance eligibility**
743,000	NISP contractors with **access to classified information**
152,453	**Requests for investigation** for security clearances processed
91,967	Interim **security clearance determinations** made
10,230	**Adverse information reports** triaged
56	Interim **Clearance suspensions** in process (actual suspensions, not LOJs)
100,000	**Knowledge Center calls** answered, providing on-the-spot personnel security clearance issue resolution

INTERNATIONAL ACTIONS

4,592	**Requests** for **Visits**
14,151	**Travelers**/Visitors
8,270	**Foreign Sites Visited**
298	**Transportation** plans
193	**Hand Carry** plans
9	**Security Vulnerability Assessments**

NISP AUTHORIZATION OFFICE

32	**NISP Command Cyber Readiness Inspections** led by DSS
4,361	System security plans **(SSPs) accepted and reviewed**

Common deficiencies in SSPs:

1. SSP not tailored to the system
2. Management Controls - SSP incomplete or missing attachments
3. Insufficient summary and description of security controls in place
4. Inaccurate Configuration Documentation

2,735	Completed **system validation visits**

Common vulnerabilities found during system validations:

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

COUNTERINTELLIGENCE

56,188	**Reports of suspicious contact** from industry
6,074	**Referrals to Law Enforcement/** Intelligence Community
734	**Investigations/operations opened** due to DSS referrals
8,023	**Intelligence Information Reports**
3,492	**Personnel** attending three **secure VTCs** with industry

CONTINUOUS EVALUATION (CE):

1,115,384	**Subjects** enrolled in CE
293,255	**Industry**
822,129	**Military Services/4th Estate**

CE Alert Reasons:

31.7%	**Financial Considerations**
31.5%	**Drug Involvement**
27.3%	**Criminal Conduct**
8.3%	**Alcohol Consumption**
1.0%	**Sexual Behavior**
0.3%	**Personal Conduct**
51	**Eligibilities Revoked** (May 2016 to December 2017)

* The CE mission and resources were realigned to the Personnel Security Management Office for Industry on Dec. 19, 2016. CE is a vetting process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated record checks and business rules to facilitate the ongoing assessment of an individual's continued eligibility.

FOREIGN OWNERSHIP, CONTROL OR INFLUENCE (FOCI)

518	**FOCI facilities**
280	**Mitigation Action Plans** in place