DSS ACCESS

Official Magazine of the Defense Security Service | **Volume 6, Issue 2**

THIS ISSUE

ISRs know the importance of partnering with industry

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: DAY IN THE LIFE OF AN ISR

INSIDE

From the Director

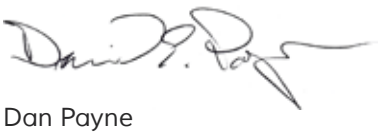
As I reviewed this issue of DSS ACCESS, I was struck by several things. First, it made me very proud to see the winners of the 2016 Director Awards highlighted in these pages. This program was instituted before my arrival at DSS, and we expanded it in 2016 with new award categories. This year's award recipients represent a true cross-section of DSS organizations and highlight the diversity and scope of the DSS mission.

In that regard, several articles in this issue bring our agency's diversity and scope into focus. We have a case study of a very complex corporate merger and our Facility Clearance Branch's proactive involvement in resolving the various issues that arose during the process. Another article features the Service Requirements Review Board, a process DSS instituted to increase visibility, collaboration, and value of services requirements throughout the agency. This is a good news story that is leading to cost and time savings agency-wide. Toward that end, I think we are all looking forward to the August launch of the National Industrial Security System. This system has been a long time coming, and I look forward to the new automation capabilities it will provide.

While our mission directorates may be on the front lines of the agency's mission, it is our supporting elements that directly enable mission success, as you can see highlighted in these pages. From observances and special events led by our Diversity and Equal Opportunity Office to Speed Mentoring sessions led by the Human Capital Management Office, DSS employees are engaged and constantly striving to make a difference.

Which brings me to my final observation relative to the article entitled Heart of a Public Servant. People don't go into government service for the pay — at least not in my experience. People choose to work for the federal government because they believe in the mission of the organization and they want to serve. Dave Bauer's article is spot on; as public servants, we have an obligation to be good and faithful stewards of the taxpayers' money. But we also have an obligation to perform our jobs to the best of our individual and organizational ability. It's clear to me that DSS employees are doing just that each and every day.

Thank you for all you do to support national security.



Dan Payne
Director

The First Line of Defense (Security Service): Industrial Security Representatives and the Importance of Industry Partnership

by Nicholas Toth
Office of Public and Legislative Affairs

The Defense Security Service (DSS) is charged with one of the most critical missions in our government: Safeguarding classified information in the hands of cleared contractors who develop the majority of the U.S.'s defense technologies. Industrial security representatives (ISRs) provide industrial security oversight and help companies with adhere to requirements outlined in the National Industrial Security Program Operating Manual (NISPOM). ISRs in the field form the backbone of DSS industrial security operations and are the point at which the rubber meets the road.

By leading DSS's industrial security oversight, ISRs serve an important function: Partnering with industry to proactively avoid, respond to, and/or mitigate industrial security risk. ISRs regularly conduct vulnerability assessments to ascertain security risk, and meet with facility security officers (FSOs) to provide "advice and assistance" on an array of issues. These issues include responding to data spills on an unsecured computer network, reporting information that may affect an employee's personnel security clearance, or providing advice on interpreting a NISPOM requirement.

In recent months, several ISRs described how they are partnering with industry to help implement policies geared toward shifting from a schedule-based model of facility prioritization to a "risk-based approach" that is driven by intelligence and focused on assets. They are also overseeing the implementation of Change 2 to the NISPOM, which requires industry to create and implement an insider threat program. Both of these initiatives have led to a substantial amount of advice and assistance contacts between the ISR and industry.

What it takes to be an effective ISR

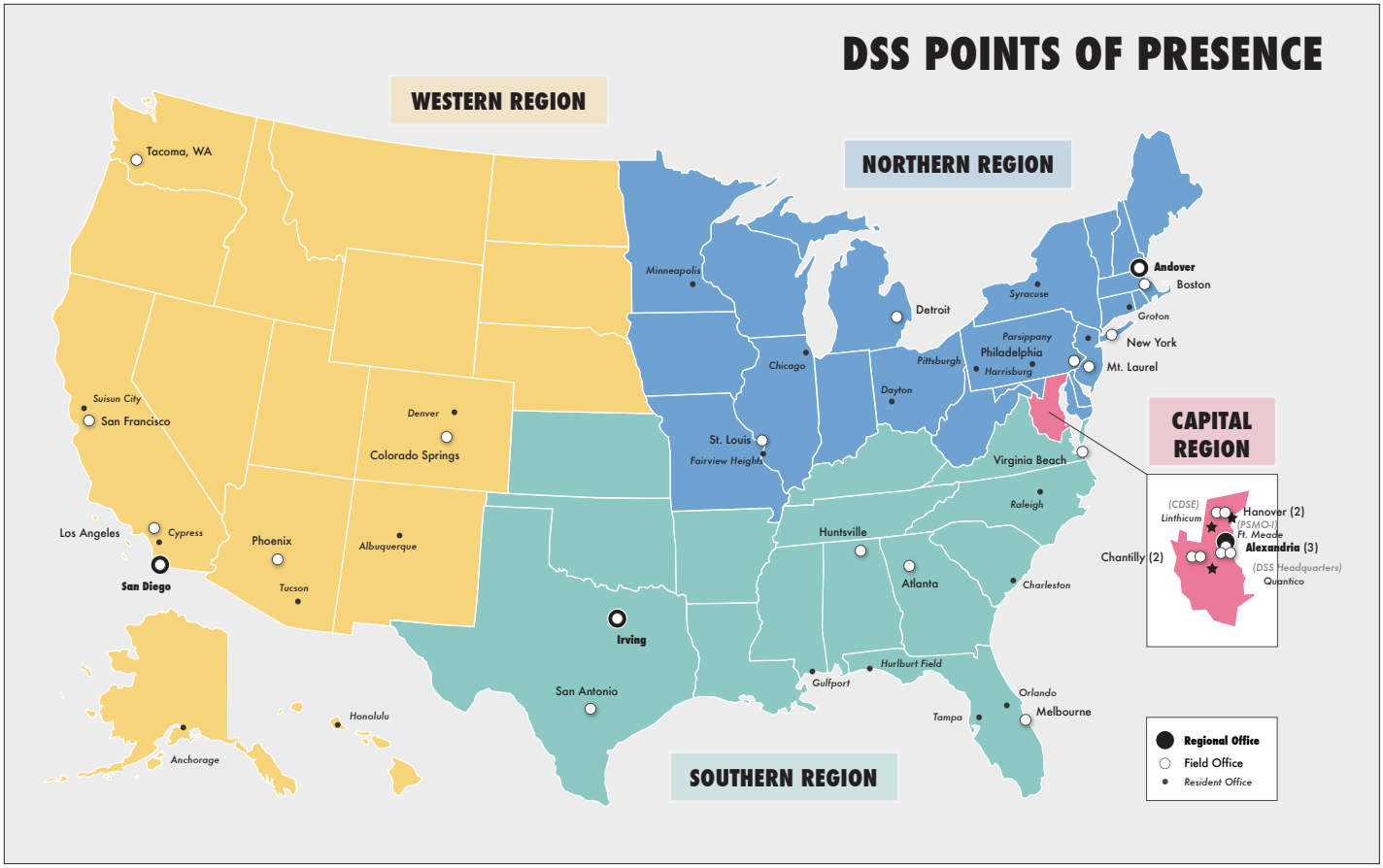
The requisite skills necessary to excel as an ISR, all of whom oversee a diverse set of facilities, cover many disciplines and competencies. Representatives are required to take a six-month National Industrial Security Program Oversight Course, which provides virtual and in-person mentoring and helps develop fundamental industrial security skills in three primary domains: Information security, physical security, and personnel security. Additionally, ISRs possess general skills, to include critical thinking, task prioritization, and the ability to build relationships and communicate effectively with industry partners. More specific skills, such as encyclopedic understanding of NISPOM policies, expertise in counterintelligence, and knowledge of business operations and structure, especially in regions where foreign ownership, control, or influence (FOCI) mitigation is common, are particularly important to the success of an ISR.

	Total FCLs	Fully Staffed ISRs	Ratio to ISR
Capital Region	4,537	59	77
Northern Region	2,537	52	49
Southern Region	2,876	46	63
Western Region	2,268	44	52
Nationally	12, 218	201	61

Regional comparisons

DSS field staff are deployed across all 50 states and located in one of four regions: Northern, Southern, Western, and Capital, comprised of 26 field offices and 21 resident offices. Field staff of approximately 201 oversee approximately 12,200 cleared facilities nationwide. The national ratio of ISR representative to facility is roughly 1:61, but varies significantly by region.

Many ISRs point out that geographical characteristics help to distinguish regions from one another. The Capital Region and the eastern portion of the Northern Region, for example, have a high concentration of smaller, less complex business



operations centers and larger corporate headquarters. The Capital Region also possesses a high density of facilities where FOCI mitigation is common. The Northern Region as a whole also contains a fair share of larger manufacturing facilities.

Joyce Pappas, Senior ISR in the Detroit Field Office, describes her area of responsibility as one that spans a "huge territory from the east coast to St. Louis and includes Detroit and Boston, which differ greatly in terms of facility characteristics" and points out that "travel distance between facilities and field offices, and weather can be a hindrance."

The Western Region is characterized as sparse and geographically spread out, and is comprised of a fairly diverse cross section of facilities ranging from small- to medium-size operations. Patricia Bourgoyne, ISR in the Albuquerque Resident Office, notes that many Native American communities own and operate facilities in her area of responsibility, which makes her region particularly unique.

Facilities located in the Southern Region encapsulate low and high density areas with many different types of facilities. The Huntsville, Ala., corridor focuses heavily on manufacturing and serves as one of the largest cleared facility hubs in the country, according to Chad Campbell, ISR in the Huntsville Field Office.

Preparing for a security vulnerability assessment

ISRs spend the bulk of their time meeting with customers and traveling to cleared facilities to conduct security vulnerability assessments (SVA). During fiscal year 2016, ISRs conducted over 5,000 SVAs nationwide. In order to prepare for an assessment, ISRs review prior assessment reports, research the Joint Personnel Adjudication System and the Industrial Security Facilities Database, review DSS counterintelligence publications, and conduct open-source research (e.g., websites, state secretaries of state filings, publicly available digital media). Regularly consulting with the information systems security professionals and Counterintelligence staff prior to a site visit helps ISRs identify other DSS concerns regarding a facility that may not be readily apparent.

On any given day, an ISR could visit a site that manufactures surface-to-air missiles, review an insider threat program at a corporate headquarters, or advise smaller "mom and pop shops" on new site construction. ISRs meet with a cross-section of company representatives, to include dedicated FSOs, corporate presidents, executive staff, program

managers, manufacturers, shipping and supply staff, or other facility contractor personnel. Facilities vary by size, type, and complexity. In smaller facilities, the owner of the company may also serve as the principal security representative; this is especially true in the Capital Region, where there are many small cleared facilities that are owned and operated by a workforce comprised of one-to-five people. In medium and large facilities, where more robust industrial security programs have been instituted, dedicated security personnel administer the company's security programs.

When ISRs are not pounding the pavement, they are often spending the bulk of their time responding to and mitigating an array of industrial security threats. Last year alone, ISRs responded to over 1,400 security violations and received nearly 40,000 suspicious contact reports from across the country. Data spills across unsecured computer networks are among the most frequent violations ISRs handle on a day-to-day basis. Unreported business structure changes stemming from a merger/acquisition, change in ownership, and suspicious contacts (e.g., spear phishing, foreign visits) are also some of the most frequent inquiries ISRs respond to.

Advice and assistance

Among their varied and important roles, ISRs regularly provide "advice and assistance" to cleared industry security personnel on a wide range of issues. During FY16, ISRs conducted over 22,000 "advise and assist visits" throughout the country. Karl Rarig, Senior ISR in the Philadelphia Field Office, believes that "providing accurate, timely and useful advice and assistance to Industry is a cornerstone of the NISP and only strengthens the partnership."

ISRs regularly encounter inquiries related to NISPOM compliance and insider threat programs, but also get less common questions as well. FSOs contact ISRs for advice on anything from preparing their employees for foreign travel to providing guidance on reporting adverse information or security violations that may affect an employee/facility security clearance. Before responding to an inquiry, ISRs will review internal DSS guidance, refer to NISPOM or relevant personnel security policies, research external sources, and then craft a response to the FSO. Industry customers may also request DSS closed area approval, request a special briefing to the FSO, or discuss how a potential change in business structure or ownership might impact the company's facility clearance.

The importance of partnership

From an outsider's perspective, the role of the ISR may be viewed as someone who assesses cleared facilities, writes citations for violators, and serves more as an "inspector" rather than a collaborator – this is far from the reality. ISRs are more interested in partnering with industry, rather than being perceived as a regulatory enforcement body. ISRs want to work with FSOs to be proactive in monitoring and reporting security issues; this is most common in facilities where ISRs engage with the FSOs through various types of formal and informal outreach efforts.

Clement LaShomb, an ISR in the Andover Field Office, points out that his office orchestrates Industry Partnership Days that brings security experts to the front door of industry partners to answer any questions or concerns they may have. When these types of relationships are established between ISRs and industry leaders, it creates a proactive environment where industry is regularly reaching out for guidance on how to best comply with the NISPOM and reduce security risk.

LaShomb believes that "timely effective communication is key in the nurturing of this proactive environment." Developing these types of relationships also help ISRs manage their workload more efficiently because they are spending focusing on responding to violations and more time working with customers on being proactive.

Some regions regularly employ creative methods to encourage DSS/Industry partnership through security education outreach. In the Western Region, ISRs sponsored two "Day with DSS" educational outreach events that provided training and education to FSOs on how to improve their threat identification skills. Following these events, ISRs in the region reported an uptick in suspicious contact reports, mostly because FSOs were able to recognize suspicious activity more easily. ISRs have also partnered with the Center for Development of Security Excellence to provide industry training on and evaluation of industry insider threats programs. These types of courses help companies tailor their required insider threat programs to meet the needs of the facility.

One of the last and arguably most important reasons why the ISR/industry partnership is so valuable is because it is the most effective way for ISRs to understand the nature of the classified activity within the facility. If an ISR does not have a clear understanding of the assets on-site, the nature and function of the operation, and the types of mechanisms used to protect classified information, the ISR will be ill-equipped to identify critical assets and assess/mitigate risk. Which reinforces the importance of ISRs partnering with industry to proactively avoid, respond to, and/or mitigate industrial security risk.

Annual award ceremony recognizes agency employees

The sixth annual Director Awards ceremony was held in early March and coincided with the annual Industrial Security Field Operations Supervisors Training. The Director Awards are presented to those employees who exhibit the highest standards of excellence, dedication, and accomplishment in support of advancing the agency's mission during the calendar year. This year DSS introduced a new category, Employee of the Year Senior – which was presented along with the Humanitarian of the Year Award; Excellence in Innovation Award, Team of the Year; and Employee of the Year.

During the event, three DSS senior leaders were recognized for their selection as Presidential Rank Award recipients. Bill Stephens, Counterintelligence Directorate, was named a Meritorious Executive, and Denise Humphrey, Center for Development of Security Excellence (CDSE), was named a Meritorious Senior Career Employee for 2016. Also recognized was Kevin Jones, CDSE, who was named a Meritorious Executive for 2012 and the first DSS employee to achieve the recognition.

In his opening remarks, Dan Payne, Director, said of the program, "it is more important than ever to keep employees engaged and demonstrate to them that their work is vital. The Director Awards Program embodies attributes that shine a light on the great work we accomplish each day," he said. "It validates the impact our products and services provide to both industry and the community; and it conveys our work ethic and dedication to the mission."

Payne noted that each individual is motivated for different reasons. "Each of us is driven by an entirely different set of motivators," he said. "Most of us perform, excel and achieve for reasons other than money, which is why we value the Director Awards Program. It conveys a genuine expression of appreciation for employee achievements and contributions to the mission."

There are two factors for which an employee or team is nominated for the Director Awards: Business results and agency core values. Business results include such factors as building partnerships, innovation, customer focus, and process improvement. Agency core values are dependability, respect, integrity, agility, collaboration, and accountability.

Payne also noted, "As we close out the 2016 Director Awards Program, we are still learning and evolving," Payne said. "We will incorporate changes that will continue to enhance the success of this program, and in turn, support the recognition of those employees who go above and beyond the call of duty."

EMPLOYEE OF THE YEAR

The Employee of the Year award is presented to the DSS employee who best exemplifies initiative, has made outstanding contributions, and whose achievement created sustainable results that most advanced the agency's mission. The winner of Employee of the Year for 2016 was Rebecca Morgan, CDSE.

Morgan was nominated for producing a strategic road map for the training and development of the insider threat program.

TOP: Employee of the Year Rebecca Morgan (right), Center for Development of Security Excellence, stands with DSS Director Dan Payne. **BOTTOM:** Employee of the Year Senior Cherry Wilcoxon (right), Financial Management, stands with DSS Director Dan Payne. (Photos by Hollie Rawl, CDSE)

Morgan forged strategic partnerships with the DSS Counterintelligence Directorate, the Office of the Under Secretary of Defense for Intelligence, National Insider Threat Task Force, and the National CI and Security Center to produce a strategic road map for development of the insider threat training program.

She worked effectively and collaboratively with stakeholders across the community to outline a five-year training initiative and secure funding. Morgan placed DSS at the forefront of the intelligence community as CDSE was named the Center of Insider Threat Training for DoD.

In accepting the award, Morgan said, "I have a little brother who is always one-upping me. While it's not a competition, we'll see if he can top this award."

She continued, "I'm a bit embarrassed to be receiving this award because it wasn't just me doing the work. I'd like to thank the leadership for acknowledging the role of training. It's not sexy. But they understood that building training in support of insider threat was a proactive way to support the security community."

Morgan noted that this is the fourth time she's worked for DSS. "I come back because of the mission, but more importantly, I come back for the people."

EMPLOYEE OF THE YEAR SENIOR

The Employee of the Year Senior award is presented to the DSS employee who exhibits the highest standards of excellence, dedication, and accomplishment in support of advancing the DSS mission. The Employee of the Year for 2016 was Cherry Wilcoxon, Financial Management Division. Wilcoxon was nominated for her efforts in the implementation of institutional reform opportunities and cost reduction targets for major headquarters.

Wilcoxon took a comprehensive review of the agency's organizational structure and masterfully devised a plan to review the staff levels of each directorate to address streamlining organizations through delayering; develop rationale for supervisory ratios; standardize position titles; and, validate manning levels, to include government civilian employee and contractor-provided services.

Her collaborative and ongoing engagement was instrumental in facilitating negotiations of the headquarters delayering and the 25 percent reduction requirements, which led to decisions favoring DSS.

In accepting the award, Wilcoxon said, "I want to thank the DSS leadership for providing me

Members of the 2016 Team of the Year, NISPOM Change 2, Insider Threat Implementation Team, stand with DSS Director Dan Payne.

the opportunity to excel. I want to thank my colleagues for their support, because I often show up unannounced and want things 'now'."

Wilcoxon continued, "And you've all heard the 'Footprints in the Sand' prayer, where during the most trying times, there was only one set of footprints because God carried the individual. Well, all I can say is that the Financial Management team carries me."

TEAM OF THE YEAR

The Team of the Year award recognizes teams who, as a group, exhibit the highest standards of excellence, dedication, and accomplishment in support of the DSS mission. The 2016 Team of the Year is the National Industrial Security Program Operating Manual (NISPOM) Change 2, Insider Threat Implementation Team.

Utilizing a "whole DSS" approach, the team flawlessly delivered the most substantive change to the NISPOM since its inception, impacting all cleared industry. The team's efforts required large-scale collaboration with industry, key government stakeholders and field representatives to develop the policy, implementation strategies and oversight plans.

2016 Team of the Year/NISPOM Change 2, Insider Threat Implementation Team members:

Ryan Deloney, Industrial Security Field Operations

Ryan Dennis, Industrial Security Field Operations

Ryan Franklin, Industrial Security Field Operations

George Goodwin, Industrial Security Integration and Application

Frank Malafarina, Counterintelligence

Keith Minard, Industrial Security Integration and Application

Rebecca Morgan, Center for Development of Security Excellence

Kyla Power, Industrial Security Field Operations

Heather Sims, Industrial Security Field Operations

The collective work of the team led to the establishment of the largest set of insider threat programs in the federal government under the oversight of a single entity. This effort represents a significant milestone in our new methodology, and its success sets an optimistic tone for the agency's progress toward a risk-based mindset.

Members of the 2016 Excellence in Innovation of the Year winners, CI Cyber Division, stand with Director Payne.

In accepting the award on behalf of the team, Ryan Deloney said, "The success of this team was critical, as the amount of damage an insider can cause today is great. This initiative wasn't limited to just one directorate, but was a whole agency effort. Representatives of each directorate were engaged as we worked early with the Office of the Secretary of Defense on change implications and timeline; we partnered with industry in the development of the Industrial Security Letter; the Center for Development of Security Excellence created some great training, with over 100,000 course completions to date; and the industrial security representatives are working with facility security officers to help establish insider threat programs.

"All these different efforts required the agency to be agile and flexible to change," he concluded.

EXCELLENCE IN INNOVATION OF THE YEAR

The Excellence in Innovation of the Year is awarded to an individual or team that develops and implements innovative products, services, processes, or technologies to meet new or existing requirements, articulate needs, and improve the way government operates. The purpose of this award is to develop new solutions that go beyond marginal improvements in existing products, services, processes or technologies. It is designed to encourage dialogue across the community, challenge peers to think and work differently, and take calculated risks to move government in a new direction.

The 2016 Excellence in Innovation of the Year was presented to Counterintelligence Cyber Division for developing and deploying a cyber intelligence tool suite which improves the dependability, quantity, and agility of technical analytic products. The division demonstrated agility in the development/

2016 Excellence in Innovation/ Counterintelligence Cyber Division members:

Jeffrey Burlette
John Kearney
John O'Halloran
Donald Reese
Ashley Smith
Christina Vargo
Derre Filipkowski
Richard Naylor
Samuel Oliver
Justin Shanken
Todd Tucker

implementation of stakeholder access to additional threat information through vastly improved cleared industry threat information sharing processes.

The team rapidly morphed from a primarily technical analysis role into well-defined roles/responsibilities of triage, technical analysis and operational engagement. As a result, the team accounted for 14 percent of DoD's measureable disruptive affect against cyber adversaries and is documented in a Defense Intelligence Agency congressional report.

In accepting the award on behalf of the team, Rich Naylor, Chief, CI Cyber Division, said, "For such a small team within DoD, they create leverage using very innovative tools. They do some phenomenal work."

He continued, "I would be remiss if I didn't thank Mr. Stephens for originally standing up the Cyber Division, and the unwavering support of Mr. Payne, Mr. Kren [Deputy Director] and the Front Office."

HUMANITARIANS OF THE YEAR

The Humanitarians of the Year award is presented to the employee or team who contributes to human welfare, and improving the quality of life and health of a group of individuals in the United States or abroad.

The employee or team nominated has demonstrated significant leadership and outstanding volunteer service accomplishments and through the scope of work undertaken a commitment to humanity and selflessness, without regard to personal or organizational gain or profit. The employee or team established or furthered a legacy and/or sustainable program that is of ongoing value and benefit to others.

The 2016 Humanitarians of the Year award was presented to two employees: Christopher Cox, CDSE, for his support to Happy Helpers for the Homeless, and Patricia Kimball, Andover Field Office, Industrial Security Field Operations, for her volunteer efforts with the Sandown Lions Club.

The 2016 Humanitarians of the Year Patricia Kimball (center), Andover Field Office, and Christopher Cox (right), Center for Development of Security Excellence, stand with Director Payne.

Christopher Cox selflessly served the homeless and at-risk community in the Baltimore area through Happy Helpers for the Homeless, a local food bank and community center. This program feeds up to 250 people, including families, every week. He also worked with Operation: Safe Escape, which focuses on the security and safety of domestic violence shelters and victims of domestic violence.

Cox demonstrates a level of dedication and commitment worthy of emulation. His actions epitomize and contribute to the well-being, safety, and comfort to those less fortunate within his community.

In accepting his award, Cox said, "One in eight people in Virginia suffer from food insecurity, and one in six in Maryland. Every individual has the opportunity to make a huge difference in someone's life."

As a part of Operation: Safe Escape, Cox works with a collection of people to enhance the safety and security of domestic violence shelters, and works to help domestic violence victims. "I'm

happy to say that we've got a 100 percent success rate in seeing those people get out of their situation," he said.

"As an individual, we can make a difference. Working together, we can make change," Cox concluded.

Patricia Kimball applied her skills in project management, budgeting, and personnel coordination to improve the quality of life for others by creating a legacy of service to her local community.

She actively volunteered her services to the Sandown Lions Club, a service organization whose goal is to build a brighter future for their community. Kimball served as the chairperson for many fundraiser dinners supporting community projects and the food pantry for Thanksgiving and Christmas baskets, and co-chaired with the church for a Veterans Day breakfast. She has been instrumental in the winter clothing drive, collecting over 500 pieces of clothing, which were donated to a local clothing pantry, homeless veteran organizations, and recently to the victims of a large apartment fire where 50 people needed winter clothing. She is not only involved with the Lions, but works with the Girl Scouts and Boy Scouts. She is also on the Old Home Days Committee and co-chaired the Old Home Day Parade giving hundreds of hours of her time. She recently received the 2016 Home Town Hero Award presented by the Granite State Communications for her community service. Her selfless dedication to her local community ensured that vital community outreach projects were effectively executed.

"I want to thank my regional director and supervisor for their recognition of my efforts, and thank my husband, who without his support, I couldn't have accomplished all that I have," Kimball said.

"We just finished collecting hundreds of articles of clothing that were donated to the homeless; hundreds of new and used books which were donated to a local hospital; and bags of glasses," she said. "When you walk by the white Lions boxes, remember that your old glasses could help someone see.

"I hope today that you walk away with a renewed sense of compassion and generosity," Kimball said. "Donate food, or drop your glasses in the white box, support those fundraiser dinners in your community because it's the little things we do that can touch those less fortunate every day."

EMPLOYEE OF THE QUARTER

Also recognized during the ceremony were the Employees of the Quarter for 2016:

First Quarter: Braden Harrison, *Industrial Security Field Operations*

Second Quarter: Sara Coonin, *Industrial Security Integration and Application*

Third Quarter: Brian Murphy, *Industrial Security Field Operations*

Fourth Quarter: Demetrius Moore, *Industrial Security Field Operations*

EMPLOYEE OF THE QUARTER

Also recognized during the ceremony were the Employees of the Quarter Senior for 2016:

Second Quarter: Stephen Heath, *Office of Acquisitions*

Third Quarter: Joseph Harne, *Industrial Security Field Operations*

Fourth Quarter: David Grogan, *Industrial Security Integration and Application*

NOMINATED FOR EMPLOYEE OF THE YEAR

Sara Coonin, Industrial Security Integration and Application, for executing the DSS vision for the risk based analysis and mitigation model.

Ashley Maddox, Headquarters, for finding innovative solutions to provide outstanding customer support.

Stephan Michaud, Counterintelligence, for impacting the DSS objective of protecting our nation's sensitive and classified programs and information by forging new partnerships with industry and government agencies.

Brian Murphy, Industrial Security Field Operations, for management of the arms, ammunition, and explosives pre-award security survey process.

NOMINATED FOR EMPLOYEE OF THE YEAR SENIOR

Timothy Barnes, Industrial Security Field Operations, for implementing innovative risk management principles.

Stephen Heath, Headquarters, for demonstrating superior leadership in ensuring innovative solutions for timely award of contracts that enabled customer mission accomplishment.

Stephen Nemeth, Industrial Security Integration and Application, for building the Business Analysis Nucleus Group into the cornerstone of the DSS risk-based analysis and mitigation initiative.

Erika Ragonese, Center for Development of Security Excellence, for developing training to support the DoD and national insider threat policies.

Robert Sirks, Counterintelligence, for identifying process improvements for the intelligence community and improving operations capability.

NOMINATED FOR TEAM OF THE YEAR

Business Analysis Nucleus Group, Industrial Security Integration and Application, for exceeding expectations with regard to facility clearance requests and foreign ownership, control or influence mitigations.

Financial Management Team, Business Enterprise, for reaching across functional boundaries to defend and secure scarce resources in order to protect the nation's cleared industrial base investment.

Leadership Advisory Board, Headquarters, for their contribution to the design of a new and innovative solution for leader development within DSS.

Special Access Program Team, Center for Development of Security Excellence, for creating six high quality videos to assist in the creation of engaging annual training throughout DoD.

Suspicious Contact Report Triage and Writing Team, Counterintelligence, for their efforts in reporting from cleared industry and their support to CI special agents.

NOMINATED FOR EXCELLENCE IN INNOVATION

Peter Jackson, Industrial Security Integration and Application, for his contribution to the Risk-Based Analysis and Mitigation approach.

Services Requirements Review Board, Business Enterprise, for reviewing all agency requirements processes and procedures, and the resources allocated to support them.

Time to Market Team, Industrial Security Field Operations, for their efforts with high profile foreign ownership, control or influence mitigation.

SENIOR LEADER ANNUAL MEETING
provides opportunity for discussion and dialogue

Even before Director Dan Payne officially joined the Defense Security Service, he attended the 2016 Senior Leader Annual Meeting (SLAM). The annual event brings together senior leaders from the field and headquarters for detailed discussions on the mission and operations of the agency as well as leadership initiatives. The 2016 SLAM was the first opportunity Payne had to meet his leadership team, and it was the their first opportunity to hear his priorities and goals for the agency.

SLAM 2017, held in March, was designed to review from a strategic standpoint the progress DSS had made in achieving Payne's goals and continuing to manage new missions and changes. In fact the theme of the three-day meeting was "Continuous Change ... Continuous Opportunity."

In his opening remarks, Payne asked for openness and honesty from his senior leaders. "Unfiltered ideas lead to good decisions and policy," he said. He continued in that vein in discussing the results of an agency climate survey conducted by the Defense Equal Opportunity Management Institute (DEOMI). The survey indicated a desire from employees for more frequent and detailed communication from the senior leaders on the agency's direction. "We have one mission," said Payne, "and that is to protect national security. Everyone is involved in that mission and contributes to it. We must all move in the same direction with the same goals. And everyone needs to understand what those are."

Payne also noted the workforce was suffering from change fatigue from the addition of new missions or responsibilities and recent legislative language that directed possible additional new missions. Payne embraced many of the new missions as providing the nation with better security, but also acknowledged the toll the constant churn had taken on the workforce. "We have to continue to focus on doing the most important stuff," said Payne, "and find other ways to do the less important stuff."

In an afternoon session, Greg Pellegrino, Principal, Strategy and Operations, Deloitte Consulting, reminded the group that strategic direction was a matter of

Regina Johnson (left), Southern Region director, talks with Dave Bauer, Western Region director, during a break at the Senior Leader Annual Meeting. (Photo by Steve Lindquist, SMO)

perspective. He encouraged the team to view strategy as a set of choices that can position DSS to achieve superior results. Pellegrino also reminded the team to focus on customer and employee experience; know the needs and expectations of the agency's customers (cleared industry/government contracting activities) as well as the needs of employees.

The remainder of the first day focused on the status of the short term goals Payne articulated in 2016. While some had been achieved such as, assignment of the unauthorized disclosure and continuous evaluation missions to DSS, it was clear the scope and resources to fully execute the new missions presented both challenges in terms of resources but also opportunities in collaboration and consolidation. Other initiatives, such as personnel security authorities for DSS counterintelligence

and DSS counterintelligence membership in the Intelligence Community remained works in progress.

On day two, Charlie Phalen, Director of the National Background Investigations Bureau (NBIB), provided an overview of NBIB during its first few months of operation. Phalen focused on the information technology enhancements underway at the fledgling organization, legacy IT systems and the labor intensive process of conducting background investigations. Phalen's presentation was followed by the Section 951 Implementation Team which provided the progress on producing two plans and one report as required by the 2017 National Defense Authorization Act (NDAA). The NDAA language directs DSS to produce these documents should Congress direct the transfer of the DoD background investigative mission from NBIB to the Department of Defense. Mike Buckley, team lead, said, "should the mission transfer, in part or in whole, it will impact every person in DSS."

The afternoon of day two focused on DSS in Transition (DiT), Payne's signature goal of developing a new, agile, responsive assessment approach to industry. Kevin Jones, lead for the effort, detailed the four steps in the new process: prioritization, asset identification, threat, vulnerability, impact analysis and review, and tailored security programs. Jones noted that integrated process teams (IPT) had been formed for each step with the goal to pilot, refine and validate the concept of operations for each. A fifth IPT was formed to identify and define working terms for DiT. Some IPTs had made more progress than others, most notably the prioritization team, which demonstrated a new automated tool for facility information. Jones emphasized that the change process was not linear with one step after another but rather, overlapping and interdependent. Jones noted that the IPTs had reached a point where further integration of effort was required to develop an overarching process and methodology, and suggested a move to a task force approach of dedicated team members to finalize the details of the transition effort.

The final day of the meeting featured a session on unconscious bias; what it is, why it matters and what to do. The session focused on encouraging participants to recognize and address unconscious bias in the workplace and how to demonstrate inclusive behavior.

The remainder of the day was devoted to a discussion of resources and the strategic environment in which DSS finds itself. Both presentations looked at external pressures on DSS such as budget constraints and how they affected the agency's ability to execute new and legacy missions. A common theme that emerged was that the globalized economy and supply chain required DSS to think strategically and examine new technology and information sources to inform decisions and ultimately, better protect cleared industry.

Payne closed the three-day session by highlighting the successes of the agency as well as the commitment of not only the senior leadership team, but also the workforce. "You make my job easy," he said. "I am proud to be part of DSS and I am excited about our mission."

Services Requirements Review Board increases collaboration, identifies value of service requirements across agency

by Christopher Kubricky
Program Integration Office

The Ike Skelton National Defense Authorization Act (NDAA) for Fiscal Year 2011 required DoD ensure that the military departments and Defense agencies establish processes for identifying, assessing, reviewing, and validating requirements for the acquisition of services. While the military departments have already implemented the Services Requirements Review Board (SRRB) review process, the DoD fourth estate agencies, to include the Defense Security Service, had not.

In early 2016, DSS implemented an interim process to review services requirements, while concurrently developing the agency SRRB regulation, which was signed in October 2016. In addition to satisfying compliance requirements, the DSS SRRB process is intended to increase visibility, collaboration, and value of services requirements throughout the agency.

Services requirements are defined as services provided to the federal government that support any new or existing effort within the organization, such as sustainment of information technology infrastructure, a new facility construction project, or personnel to support business administration functions. The SRRB allows for active management of services to ensure cost-effective, efficient application of resources to meet mission requirements.

The DSS SRRB, chaired by the agency deputy director, is comprised of the directorate heads who serve as subject matter experts to inform and assess SRRB decisions. The services requirements owners are required to attend in order to brief the SRRB on their specific requirement and when necessary, justify its execution.

The annual DSS SRRB meeting is used to review services requirements which are identified in the agency spend plan. This assures that options, renewals, and modifications have priority for acquisition purposes and promotes increased visibility for capabilities associated with new services requirements.

Outcomes of the SRRB process may include:

- the identification and elimination of similar or redundant services requirements;
- restructured resource allocations to eliminate increases to services requirements and more efficiently complete mission tasks;
- identification of new acquisition strategies to realize fiscal efficiencies;
- and identification of inherently governmental activities no longer suitable as contracted services.

Identification can lead to elimination of parts or entire contracted services capabilities when the work provided is redundant or of lower priority than other required services. Restructured resource allocations combine multiple service requirements to find operational efficiencies by implementing more efficient expectations. When similar services are identified across an agency, it is also possible to implement new acquisition strategies for increased savings.

As required by the NDAA, agencies must prepare and present the results of its SRRB to a Fourth Estate SRRB Senior Review Panel (SRP), a process managed by the Deputy Chief Management Officer. During the most recent SRP briefing, DSS successfully presented the scalable and sustainable process implemented by the agency, and validated new and emerging DSS missions through the Future Years Defense Program (FYDP). Additionally, DSS received praise for implementing and documenting the SRRB process. The SRP requested a copy of the DSS SRRB regulation and documentation template to use as the "model" for other DoD components to follow.

In FY17 the DSS SRRB process has realized $1.1 million in savings and identified areas for further analysis and increased oversight which may lead to further reductions and efficiencies through the FYDP. In FY18, the DSS SRRB process is expected to identify over $2 million in reductions and efficiencies.

Michael Stell, Colorado Springs Field Office Chief, takes notes at the annual Supervisor's Training.

AN AGENCY IN TRANSITION
focus of annual supervisors training

"Supporting DSS in Transition" was the theme for the annual Supervisors Training, held by Industrial Security Field Operations (IO) in March at DSS headquarters in Quantico, Va.

Representatives from all four regions attended the three-day training meetings, featuring an agenda packed with updates on policies, initiatives and programs. The training also included an agency update and overview by Director Dan Payne, who shared his vision for the agency in 2017.

The agenda included a number of new initiatives and updates from various working groups that will impact field operations, all with a focus on DSS in Transition. Guest speaker Heather Maloy, Ernst & Young, spoke about leading change and gaining trust, relating it to her experience at the Internal Revenue Service, where she was the former Commissioner of the Large Business and International Division. Other presentations focused on employee relations, rater consistency and SMART objectives, as well as the status of the Leadership Development Program.

Looking at a merger or acquisition at your company?

Work with DSS to ensure your facility clearance is not affected

by Amanda McGlone
Industrial Security Field Operations

Mergers, acquisitions, reorganizations, and spin-offs involving cleared companies require advanced planning to ensure a smooth transition of facility clearances and classified work. In early 2016, a large cleared company notified DSS that it planned to acquire a business sector of another large cleared company, in what would be a multibillion dollar transaction.

Given the size of the transaction, it was clear that if the transition did not go smoothly, there could be a significant risk to classified information or an inability to provide the government with the material and services needed to protect national security. The cleared companies' advanced planning and early coordination with DSS set the stage for a successful transition.

Even with this, there were still several challenges to overcome as a transaction of this size involves many moving parts. Industrial Security Field Operations took the lead on briefing internal DSS entities to include the Office of General Counsel, Industrial Security Integration and Application, Counterintelligence, and Center for the Development of Security Excellence. Meanwhile, the cleared companies held a kickoff meeting to provide more details to those same DSS offices, as well as senior managers, security teams, contracting teams, and legal representatives from both companies, and Corporate Administrative Contracting Officers (CACOs) for both sides.

As details of the transaction took shape, it was decided that it would be completed in two stages. In the first stage, the business sector being acquired would spin off from the existing cleared company. In the second stage, the now separated entity would be acquired and rebranded.

It appeared that the now rebranded organization was the same organization under a new name and legal structure, while in fact, it required a new legal entity be created. Further, the new entity needed to obtain the necessary facility clearances (FCLs) before contract novation could occur. This process of standing up a new legal entity enables a grace period in which both entities have active FCLs for contract novations and transition of security programs can occur over a period of days or weeks. Without this grace period, the FCL transfers would have to align perfectly with the transaction and contract novation dates in order to remain in compliance with the National Industrial Security Program Operating Manual.

The teams from DSS and the cleared companies worked closely over several months as the new legal entity was created, registered for Commercial and Government Entity (CAGE) codes, and completed the process to obtain FCLs. Classified contracts were then novated to the newly cleared entity within the legal structure of the acquiring cleared company, and the FCLs for the now defunct business sector were administratively terminated.

This transaction demonstrated the importance of involving DSS in discussions early on in a potential merger, acquisition, reorganization, or spin-off. It also demonstrated the breadth of impact of such a transaction, which can be seen in similar types of transactions regardless of the size. No matter the size of the companies involved, this type of transaction requires a concerted effort and coordination that may involve management, security, contracting, legal, and acquisition offices from both companies, contracting and security offices from their government or prime contract customers, and operations and policy offices from DSS. Without this effort, there is significant risk in these transactions resulting from the possibility that an uncleared company could acquire control of classified contracts, material, or assets without having the appropriate FCL or security program in place. If this occurs, existing FCLs may be invalidated and consequences to national security could be significant.

Things to consider in business transactions:
Often, companies see a transfer of people, contracts, and assets and assume the FCL will transfer as well. To most employees, it appears to be the same company under new ownership, and it may be assumed this would be a simple legal structure change. However, legally, an entirely new company may have been created. Contacting DSS early in the process to discuss the potential implication of the transaction provides an opportunity to identify potential roadblocks before they become an issue.

Cleared companies considering this type of transaction may want to ask the following questions:
Who will be working on the classified contracts post-transaction? What legal entity will employ those personnel? Does that legal entity hold a facility clearance?

If the transaction involves an entity with foreign ownership, control, or influence or a potential filing with the Committee on Foreign Investments in the United States, it becomes even more critical that parties work together early on to ensure a smooth process.

The legal implications of these transactions may differ from the NISP implications. Legally, the companies may transfer assets, but an FCL cannot be treated as an asset. A company that has not received an FCL must be assessed to ensure it meets the requirements for an FCL to serve the best interest of national security.

Will new CAGE codes be needed? If so, the company(ies) should contact Defense Logistics Agency for more information about CAGE codes. In general, just like FCLs, CAGE codes are issued to a legal entity. If that legal entity does a legal name change or conversion, the CAGE code and FCL may remain with the entity. If the existing entity is dissolved or remains in place as a separate organization and a new legal entity takes control of classified contracts, the new legal entity may also need a new CAGE code.

What type of coordination will need to be accomplished with CACOs and customers to ensure contracts will transition smoothly? When contract novation is required, contracts often need to be novated to a cleared company with an active FCL from a cleared company with an active FCL to prevent any interruption of work or risk to classified information.

Does this affect multiple FCLs? Are there branch offices or multiple subsidiaries that may be impacted? If so, different processes may be necessary for FCLs

under different scenarios. The company(ies) should designate a single point of contact to ensure consistent communication and tracking of all impacted FCLs.

Lessons Learned
Early and frequent communication with DSS is critical. In this case, communication began before the exact details of the transaction were even known. This was essential to ensure all the potential impacts of the planned transaction were considered and advanced action could occur to mitigate risk. There is often a fine line between a minor change condition and a major transaction that requires new FCLs. Cleared companies should provide as much information as possible about their plan to DSS as often as possible. It is essential that key management personnel of cleared companies be aware of the potential impacts of this type of transaction so they can be brought to the attention of the facility security officer and DSS. Likewise, it is essential for DSS to involve the right offices and directorates, and communicate across them.

Additionally, designating a single point of contact at DSS is often best to ensure consistent communication and resource alignment. The DSS point of contact will usually be an industrial security representative with primary responsibility/awareness of the company(ies) contracts and security program(s).

Cyber standards added to security skill set

by Stephanie Fox
Center for Development of Security Excellence

The DoD Security Training Council (DSTC) approved cyber standards for inclusion in the DoD Security Skill Standards, which documents and codifies the Department's expectations of what a security professional needs to know and be able to do to protect the nation's assets. While security professionals seek to understand how cyber affects their job roles, these standards also affect certification assessments under the Security Professional Education Development (SPēD) Certification Program.

What Changed: SPēD Certifications

Along with these updated standards came changes to the Security Fundamentals Professional Certification (SFPC) and the Security Asset Protection Professional Certification (SAPPC) assessments, which measure knowledge- and application-level standards, respectively. The SPēD Certification Program will integrate cyber standards into these certifications' assessments on Oct. 2, 2017, and will release updates to the Candidate Handbook and review material at least 30 days prior to this integration.

What Changed: Knowledge Level ("needs to know")

A security professional will identify fundamental cyber concepts.

- Ensure proactive and continuous engagement and collaboration between security, information technology (IT), and cyber professionals
- Provide timely and relevant classification direction, secure physical environment, and appropriately-cleared users in support of the DoD Certification and Accreditation processes to meet mission requirements
- Address unauthorized disclosures of information, including notifications, inquiry/investigation, and damage assessment
- Clarify whether a security incident has actually occurred upon notification of a data spill
- Identify new risks and develop appropriate procedures to mitigate those risks for new technology and equipment
- Ensure classified information is properly marked, regardless of media
- Consider the potential for creation of classified compilations when reviewing internet postings, new IT systems, and security classification guidance

Cluster	Area of Expertise	Sub-Topic
Information Security	Cyber for Professionals	Cyber and Information Security Concepts
General Security	Cyber for Professionals	Risk Management Framework
		IT/IS Security Functionality and Controls
		Inspections and Assessments

Information Security	Cyber for Professionals	Cyber and Information Security Concepts
General Security	Cyber for Professionals	Risk Management Framework
		Inspections and Assessments

TOP: Changes and Additions to SFPC Areas of Expertise
BOTTOM: Changes and Additions to SAPPC Areas of Expertise

What Changed: Application Level ("needs to be able to do")

A security professional will examine their role in protecting DoD information systems and technology.

- Provide timely and relevant classification direction in support of the DoD IT Assessment and Authorization process
- Support processes for addressing issues that affect the status of or changes to personnel's eligibility for a security clearance
- Work proactively with information system stakeholders and cybersecurity professionals to identify and assess risks to existing and new information systems, technology, and equipment
- Implement measures for mitigating risks associated with the introduction of new technology and equipment
- Support development of System Security Plans and Assessment and Authorization packages
- Enact actions that facilitate the effective handling of security incidents, including leading response to information spills
- Incorporate measures governing the proper use of social networking services

For more information, including additional updates as the program implements these new standards, please visit **http://www.cdse.edu/certification/**.

After collaborative effort, National Industrial Security System will deploy this summer

by Ryan Deloney
Industrial Security Field Operations

After more than a year in development, the National Industrial Security System (NISS) will deploy In August 2017, with a two-month "soft launch."

The NISS is the new DSS information system that will replace and expand on the capabilities of the Industrial Security Facilities Database (ISFD) and Electronic Facilities Clearance System (e-FCL), and provide an on-demand, data-driven environment with automated workflows accessible to both industry and government. NISS was developed through a collaboration between DSS, industry and government partners.

The deployment process provides users a time frame to access and get familiar with the new system and ensure a seamless transition from ISFD/e-FCL to NISS. Between August and October, NISS will be available for users to register their accounts through the NISP Central Access Information Security System (NCAISS), access the system, test capabilities, conduct training, and provide feedback. Users will be encouraged to explore the system and its capabilities.

During these two months, ISFD and e-FCL will continue to be used as the systems of record for facility clearance information. In October, at the end of the soft launch period, ISFD and e-FCL will be shut down and data migrated to NISS, with NISS then serving as the system of record for facility clearances.

The initial deployment of NISS will provide key capabilities, to include:

- Submit and view progress of facility clearance sponsorship requests
- Automatically receive notifications for key events, such as updates to facility clearance status or a change in assigned industrial security representative
- Access a knowledge base with system related content and links to relevant external information
- View For Official Use Only notices, such as cyber threat bulletins
- View new and archived DSS information, such as the Voice of Industry Newsletter
- Overall improved timelines for DSS processing through automated workflows
- Single sign-on, role-based access through NCAISS

Industry partners will have additional benefits, to include:

- Submit and view progress on facility clearance documentation packages
- Submit and view progress on reportable facility change conditions
- Submit annual self-inspection certifications
- Message assigned industrial security representative (to include sending security violations, suspicious contact reports, and other content)
- View and submit updates on facility information (DSS facility data such as holdings, programs, key management personnel, foreign ownership, control, or influence information, etc.)
- Complete surveys such as the Personnel Security Investigation (PSI) Projection Survey

A web-based training course on the NISS will be available through the Security Training, Education, and Professionalization Portal (STEPP). Additionally, webinars on NISS functionality will be provided throughout the year and accessible to all interested parties.

Automation enhancements won't stop with the deployment of NISS this year. There are planned quarterly releases and major incremental enhancements for 2018 and beyond that will provide additional smart-forms, automation, information availability, and mobile capabilities. Within the NISS, users will be able to provide feedback on system functionality and directly request enhancements. Feedback will be prioritized and deployed to improve user experience and facilitate a risk-based approach to administer the National Industrial Security Program (NISP).

More information can be found on the DSS homepage under Information Systems – NISS.

A Q&A with **Rich Naylor**, Deputy Director of Cybersecurity Operations, Counterintelligence Directorate

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

Rich Naylor is responsible for executing DSS' cyber operations in the National Industrial Security Program. He joined DSS in September 2011 as the Chief, Cybersecurity Division.

Prior to joining DSS, he was the Deputy Director, Communications, Computers, Architectures and Chief Information Officer, U.S. Cyber Command.

A retired Air Force colonel, Naylor had a distinguished military career and served in a variety of organizations, to include: U.S. Space Command, Air Force Office of Special Investigations and U.S. Special Operations Command, before retiring in 2011. Naylor was twice selected to command and served as a numbered Air Force vice commander. He is the recipient of numerous military decorations, including the Defense Superior Service Medal and two awards of the Legion of Merit.

Q: Tell us about your background and how you came to DSS and this position.

I consider myself very fortunate to have joined the DSS team. Former Director Stan Sims had worked for my boss at the time, Gen. Keith Alexander, commander, U.S. Cyber Command. Mr. Sims called him in search of a cyber expert who might be interested in DSS, and I was encouraged to explore the idea. Frankly, I knew little of DSS. However, it didn't take long to realize DSS' particularly unique and important charge. During the many interviews and discussions with the Director, his and the senior leaderships' passion for protecting our nation's assets were infectious. It seemed equally clear that as DoD was increasingly becoming a hard cyber target, our adversaries would ramp up their leverage of the cyber domain against contractors; hence DSS would be the place to be. If in some way my years of cyber operations could benefit this mission, it became the place I wanted to be.

Q: Your position at DSS was a new one when you arrived. What was the original vision for the position?

Initially entering DSS, the Director gave me a simple charge, "How will the cyber domain impact the National Industrial Security Program, and how will we adapt."

Q: What was the biggest challenge on day one?

The largest challenge has been driving the understanding that "unclassified" is not equal to no threat. Just like in land, sea, air and space, adversarial actions in the cyber domain, regardless of the classification, present similar and domain-unique concerns. Initially the belief that the unclassified cyber domain had no bearing on the protection of classified programs and cleared individuals was a common misperception. Fortunately, much of that misperception has been overcome, and the correction inculcated in publications like Change 2 to the National Industrial Security Program Operating Manual and Industrial Security Letter 2013-05, "contractors must report activities that otherwise meet the thresholds for reporting, including activities that may have occurred on its unclassified systems."

Q: What is the current mission/vision of Cybersecurity Operations?

The Director's Annual Guidance, dated April 8, 2016, states under Defense Security Enterprise Transformation, "Identify and counter foreign intelligence cyber activities through support to national-level cyber initiatives and collaboration with government organizations and key partners." Additionally, the Director and Executive Steering Committee have overwhelmingly approved the first update to DSS Strategic Plan 2020. This raises DSS' cyber focus

across the entire agency, with the new strategic objective of, "*Innovate and implement cyberspace effects.*" It also includes four performance goals: 1) *Inculcate cyberspace learning that drives the full range of cyberspace activities;* 2) *Create and evolve capabilities to enhance effectiveness in cyberspace;* 3) *Implement agile and enduring cyberspace solutions;* and 4) *Develop cyber policy.*"

The really cool part is DSS has turned the corner on leveraging the cyber domain to its advantage as we operationalize it.

Q: How does your mission align with that of the National Industrial Security Program Authorization Office (NAO)? Are they complementary?

Cyber Operations, NAO and the Office of the Chief Information Officer's Computer Network Defense all work together within our unique realms; in essence, we inform each other's mission sets.

Q: How will your office support the new DSS methodology?

I'll reverse the question, it would be virtually impossible to address risk without addressing the impact, perils, threats and vulnerabilities presented by the cyber domain.

Q: Cyber is in the news all the time, what do you see as the biggest challenges your team faces? And what do you see for the future?

Given our size and limited resources compared to those of our adversaries, overlaid on the vastness of the cleared contractor base, it's apparent that we have to innovate. The task of thwarting our cyber-based adversaries sounds overwhelming, but I am optimistic. Recently the Cyber Division was awarded the agency's team of the year for innovation award for developing and bringing the Cyber Intelligence Tool Suite (CITS) to an operational capability. CITS represents a foray into the future of how we can leverage the cyber domain to proactively predict adversarial actions. However, quoting Robert Frost, we have "miles to go before I [we] sleep, and miles to go before I [we] sleep."

DSS employees were once again generous during this year's Combined Federal Campaign (CFC) and "showed some love"

The Department of Defense raised more than $14 million for the CFC this year, surpassing its $9 million goal by more than $5 million. This made DoD the highest-achieving federal agency in the 2016 campaign. At an award ceremony hosted by Bob Work, Deputy Secretary of Defense, the Capital Region was awarded the Summit Award for collecting at least three percent more donations then the previous year. The Capital Region collected $8,000, far exceeding its goal of $5,000. In the photo at right is (from left to right) DEPSECDEF Work; Troy Littles, DSS Chief of Staff; Anne Snellings, Industrial Security Integration & Application and the agency CFC campaign manager; Rosie Allen-Herring, president and chief executive officer of United Way of the National Capital Area; and Michael Rhodes, director of administration and management in the Office of the Secretary of Defense.

The Western Region exceeded its goal by 144 percent, collecting $14,496; and the San Francisco Field Office received the CFC Gold Star Award at the Northern California 2016 CFC Awards Celebration at NASA Ames Research Center, Calif. In the photo above, Field Office Chief Kevin Flowers (second from left), and Senior Industrial Security Representative Juaquita Gray (second from right) receive the award. NorCal agencies raised over $2.76 million. Of the approximately 1,800 Federal entities involved in the campaign, the San Francisco Field Office was in the top two percent for average gifts to CFC; and in the "DoD other than Military" category, the field office was the number one entity for average gift contributions. Industrial Security Representative June Kim was the field office CFC coordinator.

Celebrating Black History Month

Dr. Evie Terrono (in photo below), professor of art history at Randolph-Macon College, spoke at the DSS 2017 Black History Month celebration in February. The theme for the celebration was "Civil War to Civil Rights: How African American Artists Engage the Past." Terrono provided several examples of African-American artists and how their work reflected the social movement of the time. Vocalist DC Washington sang the national anthem and a bluesy rendition of "Lean On Me." In the photo at left, Chris Morton (right), Office of the Chief Information Officer, speaks with Terrono after the presentation. (Photos by Marc Pulliam, CDSE)

Hold each other accountable

Call of public service can be lost in day-to-day demands

by Dave Bauer
Director, Western Region

Editor's note: *The following is a first-hand account of an experience of a DSS employee. The event caused him to reflect on the nature of the DSS mission as well as the role of public servant. The article reflects his thoughts and opinions.*

Recently, I attended a security vulnerability assessment exit briefing for a cleared company that received an unsatisfactory rating of their security program. While I knew the cleared company would be disappointed with their rating, I was surprised by the tension in the room as we presented our findings. I had heard stories of difficult exit briefings that turned hostile, but I always supposed these events were exaggerated or embellished to make the story more memorable. During the exit briefing, I suggested the government customer had entrusted both DSS and the cleared contractor with its national defense information and the evaluation revealed we had failed to meet those expectations. After the briefing concluded, I was left wondering how our national security partnership with cleared industry and mutual devotion to the goal of protecting national security could be viewed so differently.

Fortunately, this event is the exception and not the norm in the DSS and cleared industry partnership. Every day, DSS and industry work together to ensure the protection of national defense information and we continue to strengthen that partnership with the common goal of protecting our technological, military and economic well-being. However, I gained a deeper appreciation for what DSS personnel can face when living up to their responsibility as public servants, even when it is uncomfortable or controversial. I reflected on the unique nature of a public servant within the context of the National Industrial Security Program. Here are a few overarching ideas to consider:

- The importance and urgency of the mission: The DSS mission statement includes powerful descriptions, such as "strengthens national security at home and abroad" and "oversees the protection of U.S. and foreign classified information and technologies in the hands of cleared industry." DSS's Strategic Plan 2020 identified the nation as a key stakeholder, claiming DSS "contributes to national security for the common good of the nation." Simply stated, DSS does not exist for its own self-benefit but for the protection of our nation. The public trust and the seriousness of our mission demand every person devote themselves to performing the mission to the best of their abilities and to work with our stakeholders toward the best outcome for the nation.

- Nation's welfare over self-interest: DSS employees have chosen a career devoted to public service over their own self interest. Public servants are prohibited from using their authority, title, and personnel for their own personal benefit. When we engage with cleared industry and our government partners, every DSS employee must pursue what is best for national security over any self-interest, to include personal gain, embarrassment or disagreement.

- Respecting Congress' role and direction: Public servants must not "undermine or nullify the will of the legislature (Congress) in pursuit of their own views of the public interest." We DO have a responsibility to identify problems, streamline processes, and stop waste and fraud. When

confronted with challenges that seem to place Congressional direction at odds with your better judgment, every Federal employee has the responsibility to raise the issues immediately and seek reform. Still, as we work within the government system to seek appropriate recourse, we must respect the legislative intent and the interpretations of those senior leaders appointed above us.

- Setting a good example in our actions: Public servants must not act out of malice or administer unfair punishment to damage others. We must always use our independent and objective judgment to decide matters based on their merits, without bias or favoritism. As public servants, we are entrusted with important responsibilities that are inherently governmental and cannot be delegated to another person or interest. We must guard our every action in the light of our concern for safeguarding the public trust.

- Public accountability: DSS, as with other government agencies, must exercise our authorities in a way that can stand up to public scrutiny. There are certain aspects of our jobs that must be protected from the public disclosure in the interests of national security. In those cases, the conduct of our agency and each person must adhere to the highest standards of conduct and inspection by the appropriate governmental oversight organizations.

- Personal accountability: DSS employees must strive to be informed, honest, and responsive to the needs of our stakeholders (the nation, cleared industry, government customers, and intelligence and security communities). DSS has a huge mission with only so many resources, and the partnership with industry hinges on our commitment to be experts in our craft, fair, transparent, and available. Industry is counting on our being objective, clear, discerning experts. At the end of each workday, I hope to answer yes to the question: Did you do your part to make the nation safer today?

When I take time to consider higher public service ideals, it serves as a convincing and humbling reminder that the call of public service can be lost in the day-to-day demands of daily life. I know I have not mastered self-discipline in all aspects of my own behavior and conduct, but as public servants, we must pursue the ideals of public service every day. We can hold each other accountable to the greater ideal of what is in the spirit of the common good and the great responsibility entrusted to us.

Enhancing employee retention goal of second speed mentoring event

by Israel Seda-Sanchez
Human Capital Management Office

Retaining a motivated workforce is critical to the success of any organization, yet staff retention presents a common challenge for agencies nationwide. Mentoring programs have been explored as one method of creating environments that promote staff engagement and productivity. Mentoring relationships within the federal government, provide ongoing interactions, coaching, teaching, and role modeling to facilitate workforce progression along this continuum. From increased morale to enhanced career development, the benefits to an organization that actively supports mentoring are numerous.

Recognizing the importance of employee retention, DSS is working to establish a culture that fosters informal mentoring at all grade levels. In February, the Human Capital Management Office (HCMO) hosted its second Speed Mentoring event at the DSS headquarters. Senior executives and emerging leaders had the opportunity to circulate and discuss career goals, personal concerns, and professional challenges with other employees at all grade levels. This event was part of the agency's 'retention toolbox' that supports reduction of the agency's attrition rate, and retention of its highly skilled and diverse workforce.

Based on feedback its first speed mentoring event, HCMO made significant changes to the program. This year two separate sessions were held, accommodating a larger number of employees. The number of minutes per session was increased from three to seven, and mentors and mentees were aligned according to grade. Senior executives mentored GG-15s and GG-14s in the morning session which had nine mentors and nine mentees; and senior professionals mentored GG-13s and below in the afternoon session, which had nine mentors and 14 mentees participating.

The speedy event allowed mentees to receive multiple inputs on personal and professional issues while, simultaneously, providing the opportunity to network with senior leaders in hopes of establishing future mentoring relationships.

David Grogan, Industrial Security Integration & Application directorate, offers career tips during the Speed Mentoring. (Photos by Beth Alber, OPLA)

Laura Szadvari, HCMO Recruitment manager, closed the program with a quote from film director Steven Spielberg, "The delicate balance of mentoring someone is not creating them in your own image, but giving them the opportunity to create themselves."

Both mentors and mentees declared the event a success. They appreciated the time spent and knowledge shared, as indicated by feedback from two of the mentees who participated.

"I came in a skeptic, and am leaving as a supporter. I will encourage this to everyone. More people need to take advantage of this."

"Keep it up. More people need to hear about what our leadership has to provide. They provided great guidance, and the good thing is I didn't hear the same information twice."

In response to such encouraging feedback, HCMO will lead a similar initiative this summer, focusing on mentees at DSS field offices across the nation. Establishing informal mentor relationships among staff is one method that offers the support and nurturing needed for agency success and advancement of the DSS mission.

TOP LEFT: Stephanie Courtney, Freedom of Information and Privacy Act Office, asks a question during the Speed Mentoring event. **TOP RIGHT:** James Fulmer, Human Capital Management Office, focuses on his mentee at the Speed Mentoring Event. **BOTTOM:** Naimah Thompson, Program Integration Office, explains options for career development during the Speed Mentoring.

DSS KIDS TAKE OVER

Almost 400 children, 90 from the Defense Security Service alone, descended on the Russell-Knox Building on April 27, 2017 for the annual Take Your Child to Work Day event. The day-long event kicked off with a formal ceremony and pledge of allegiance. In his opening remarks, Fred Gortler, Director, Industrial Security Integration and Application, said that the event theme, "Count on Us," applies in work and play, that it takes all of us working together to accomplish even the smallest task.

The children were then divided into age groups and followed separate but similar agendas for the day. Each age group toured the DSS Data Center, internet and social media security.

The day concluded with military martial arts and working dog demonstrations, as well as static displays of military and first responder vehicles and equipment.

These photos show various activities held during the RKB Take Your Child to Work Day.

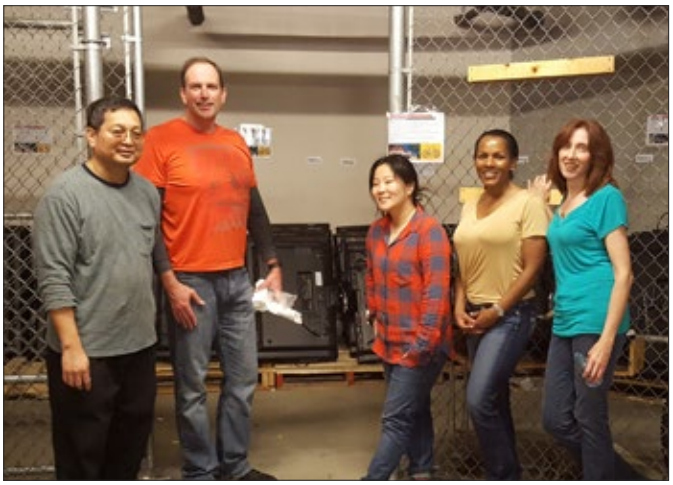
San Francisco Field Office supports local program

In February 2017, members of the San Francisco Field Office volunteered their time in support of the Ronald McDonald House, Stanford, Calif.

Field office volunteers' unpacked 67 televisions, broke down and discarded the boxes, and placed the TVs in a secure area to be installed at a later time. The effort yielded a fun afternoon for the field office but also contributed to creating a comfortable environment so that families can focus on what matters most - the health and well-being of their children.

It was a personal choice for the field office in supporting the Ronald McDonald House because Field Office Chief Kevin Flowers stayed at such a facility while his daughter underwent cancer treatments for leukemia. The field office realized first-hand that it can make a difference by giving support and providing comfort, hope, and joy to families facing medical emergencies.

The mission of the Ronald McDonald House is to create a home-away-from-home for families with critically ill children undergoing treatment at local hospitals. The house in Stanford currently accommodates 67 families with private bedrooms. Volunteers are vital to the creation of a home-away-from-home atmosphere for families of children with life-threatening illnesses.



Members of the San Francisco Field Office stands in the area where the TVs they've unpacked for Ronald McDonald House will be stored.

DSS employee retires after 38 years of service

After 38 years of working with the Defense Security Service, Donna Walker, Field Office Chief in the Detroit Field Office, retired in December 2016.

Walker started her career with DSS in 1978 as a special agent supporting the Personnel Security Investigations mission, later serving as an industrial security representative and operations manager prior to serving as the Detroit Field Office Chief in July 2000.

During her time with DSS, she also served as the acting director of the Northern Region for six months in 2009, and as acting Field Office Chief in the Sunnyvale, Atlanta, and St. Louis field offices.

At her retirement ceremony, Walker received the Distinguished Service Award for exemplary performance and significant contributions to DSS from March 1978 through December 2016. She also received a United States flag, which was flown over the United States Capitol at the request of the Honorable Debbie Stabenow, U.S. Senator for Michigan.

Donna Walker (center), Detroit Field Office Chief, stands with Mike Halter (left), Industrial Security Field Operations Deputy Director, and Cheryl Matthew, Northern Region Director, at her retirement ceremony.