DSS ACCESS

Official Magazine of the Defense Security Service | **Volume 7, Issue 3**

THIS ISSUE

Agency recognizes the best in industrial 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

Executive Director | Troy Littles

Chief, Public Affairs |
Cindy McGovern

Editor | Elizabeth Alber

Layout and Graphics |
Marc Pulliam

DSS ACCESS is an authorized agency information publication, published for employees of the Defense Security Service and members of the defense security and intelligence communities.

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

All pictures are DoD photos, unless otherwise identified.

COVER STORY: AGENCY RECOGNIZES THE BEST IN INDUSTRIAL SECURITY

DSS honors the best in industrial security; 39 facilities receive Cogswell Awards 4

In their own words 6

INSIDE

DSS employees receive awards at NCMS training seminar 18

22nd Annual FOCI Conference: Developing a DSS playbook for staging victory in industrial security 20

Oklahoma City Remembrance
'The spirit of this city and this nation will not be defeated' 24

Next generation training delivery platform enhances current system 26

Focus of Operation Training Events is to improve DiT understanding 27

'Empowering the next generation' focus of mentoring conference 28

DSS welcomes new senior leaders 29

Nammo Talley wins excellence in counterintelligence award 30

CDSE receives multiple awards in recognition of its efforts 31

DSS employee completes Harvard Program 32

DSS employees receive counterintelligence and security awards 33

Program manager authors book to help organizations improve customer service 35

ASK THE LEADERSHIP

A Q&A with Cherry L. Wilcoxon, Chief Financial Officer 22

From the Director

I am pleased to share our annual Cogswell Award issue with you. For the past several years, we have invited a cross section of our Cogswell winners to contribute articles that highlight their security programs and their success. We do this to share best practices, lessons learned and tried-and-true methods to achieve outstanding results. When I read the articles, I was struck by the strength of the relationship the facilities had with their DSS representatives. They shared information, discussed problems and issues as they arose, and rather than relying strictly on the NISPOM, looked for innovative and creative solutions. It's clear that our partnership with industry is strong, and our shift from a compliance-based assessment approach to a holistic, risk-based approach is the right one. I encourage our industry partners to read these articles and see what you can leverage to enhance your security program. Congratulations to all the Cogswell winners!

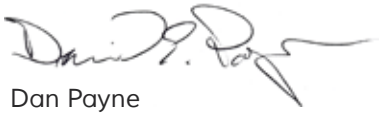
In my last column, I talked briefly about the background investigation mission and its pending realignment to DSS. While the details and timing of the transfer remain fluid, I want to touch on the latest information. On June 21, 2018, the White House announced its intent to keep the background investigative program intact and under a single organizational banner, transferring the entire mission from the Office of Personnel Management's National Background Investigations Bureau (NBIB) to the Department of Defense/DSS. This proposal was just one recommendation under a comprehensive Executive branch reorganization.

The transfer would apply to all investigations NBIB conducts, as well as the entirety of NBIB's workforce, assets and resources. This will avoid a variety of potential problems inherent in splitting the existing program into two pieces, and provides the means to achieve bold, transformative reform in how background investigations are conducted.

For several months, DSS and NBIB have been working closely to execute the legislation. Though the effective date is yet to be determined, we're using our established working groups to prepare to accomplish this transfer quickly and efficiently.

It is important for everyone to understand that with the consolidation of this mission in DoD, we collectively have an unprecedented opportunity to modernize and reform background investigations across the Federal Government. A strong NBIB-DoD team is our best combination for success. My goal, in partnership with NBIB, is to ensure this transfer is seamless and transparent, and to avoid interruptions to our missions or impact to our customers.

Thank you for all you do.



Dan Payne
Director

DSS honors the best in industrial security; 39 facilities receive

COGSWELL AWARDS

by Beth Alber
Office of Public and Legislative Affairs

On June 6, 2018, the Defense Security Service presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 39 cleared contractor facilities during the 54th annual NCMS training seminar in Dallas, Texas. The Cogswell awards represent the "best of the best," and the winning facilities' security programs stand as models for others to emulate. These 39 facilities represent less than one-tenth of one percent of the over 13,000 cleared facilities in the National Industrial Security Program (NISP).

Each year, DSS partners with NCMS to host the Cogswell Award presentations during its annual training seminar. DSS Director Dan Payne noted that for 54 years, NCMS has been delivering security education and providing training forums that align with DSS; has been bringing security professionals together to learn from each other; and has been building bridges between government and industry security professionals. "NCMS and DSS have had a long-standing relationship since NCMS' establishment," Payne said, "and we want to continue to maintain this relationship with the hope of impacting our nation in a greater way."

Matt Roche, Industrial Security Field Operations, reads the list of Cogswell winners at the award ceremony. (Photo courtesy of NCMS)

The Cogswell Award was established in 1966 in honor of the late Air Force Col. James S. Cogswell, who articulated the underlying principle of the Industrial Security Program — the need for a true partnership between industry and government to ensure the protection of classified information, materials, and programs.

During his remarks, Payne described the Cogswell selection process as rigorous. The process begins with a DSS industrial security representative who nominates a facility. That facility must have achieved two consecutive superior ratings just to be considered for the award. "This just gets you in the door, but also demonstrates a consistent, committed program over time," Payne said.

Once nominated, the facility enters an eight-month DSS internal review process that includes a National Review Team of DSS regional directors and representatives from across DSS who consider each nomination. The National Review Team vets all nominations with 57 external agencies and makes recommendations to DSS senior leadership for a final decision based upon the following criteria:

- Overall security program
- Senior management support
- Security vulnerability assessments
- Security education and awareness
- Facility security officer and security staff level of experience
- Classified material controls

In closing, Payne said, "The rigorous selection process shows you just how hard it is to achieve this honor and the significance of the achievement. It demonstrates the commitment of the awardees in maintaining the highest standard in securing our nation's assets."

Congratulations to the

2018 COGSWELL AWARD WINNERS!

Accenture Federal Services, LLC
Arlington, Va.

Accenture Federal Services, LLC
San Diego, Calif.

Applied Research Associates, Inc.
Raleigh, N.C.

Argon ST, Inc.
Fairfax, Va.

BAE Systems Information & Electronic Systems Integration, Inc.
Arlington, Va.

BAE Systems Information & Electronic Systems Integration, Inc.
Hudson, N.H.

BAE Systems Information & Electronic Systems Integration, Inc.
Merrimack, N.H.

BAE Systems Information & Electronic Systems Integration, Inc.
Nashua, N.H.

BAE Systems Technology Solutions & Services, Inc.
Mount Laurel, N.J.

Boeing Aerospace Operations, Inc.
San Antonio, Texas

DRS Global Enterprise Solutions, Inc.
Tampa, Fla.

DRS Network & Imaging Systems, LLC
Dallas, Texas

Espey Manufacturing and Electronics Corp.
Saratoga Springs, N.Y.

Gryphon Technologies, L.C., Crane Division
Bloomington, Ind.

Harris Corporation
Clifton, N.J.

Intuitive Research and Technology Corporation
Huntsville, Ala.

Jacobs Technology, Inc.
Tampa, Fla.

L3 Technologies, AMI Instruments
Broken Arrow, Okla.

Leidos, Inc.
Reston, Va.

Lockheed Martin Corporation – LM Aeronautics Company
Fort Worth, Texas

Lockheed Martin Corporation – Maritime Systems & Sensors
Riviera Beach, Fla.

Lockheed Martin Corporation – Missiles & Fire Control
Troy, Ala.

Lockheed Martin Rotary and Mission Systems
Akron, Ohio

Lockheed Martin Rotary and Mission Systems
Washington, D.C.

MBDA Incorporated
Arlington, Va.

Nammo Talley, Inc.
Mesa, Ariz.

Northrop Grumman Corporation – UMS Center
Moss Point, Miss.

Palantir USG, Inc.
Palo Alto, Calif.

Palantir USG, Inc. – DC Office
Washington, D.C.

Quantics, Inc.
Exton, Penn.

Raytheon Applied Signal Technology, Inc.
Sunnyvale, Calif.

Raytheon Company
Chesapeake, Va.

Raytheon Company
Arlington, Va.

Raytheon Company – Missile Defense Center
Woburn, Mass.

Serco Services, Inc.
Colorado Springs, Colo.

Serco, Inc.
Reston, Va.

Teledyne Scientific & Imaging, LLC
Thousand Oaks, Calif.

The University of Alabama in Huntsville
Huntsville, Ala.

Worldwide Language Resources, LLC
Fayetteville, N.C.

IN THEIR OWN WORDS

A representative sampling of the 2018 Cogswell winners were invited to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high quality security posture.

Accenture Federal Services

by Bob Grimsland
Corporate Facility Security Officer
Accenture Federal Services, Arlington, Va.

As a 40-year career security officer with federal and private sector security experience, I was honored and very proud to accept the 2018 Defense Security Service Cogswell Award on behalf of my associates at **Accenture Federal Services** (AFS) for our Arlington, Va., facility. I was joined in Dallas by my colleague, Amaneece (Aimee) Harrison, our facility security officer in San Diego, who accepted a Cogswell Award for that facility, as well. These awards reflect the hard work, dedication, and commitment of our entire security team and all AFS employees across our enterprise. We view security as a team effort within AFS. In fact, our "One Team Approach" is part of our strategic vision and a goal we continually strive to accomplish.

As I reflect on the two awards, there are many factors that contributed to our success. These factors are valid for all successful security programs whether in the federal or private sector. Below are a few of the more critical ones:

Integrated and collaborative security workforce
Our security workforce is the single most significant factor in our success this year. I am proud to work with such a group of dedicated professionals. However, dedication and hard work is not enough. Our Chief Security Officer Brian Prioletti, and our Chief Information Security Officer Nicole Dean are consistently advocating to provide an integrated, collaborative security product to our clients and stakeholders. I know from experience that it's very easy to become "stovepiped" in our unique functional security disciplines. With today's increasing threats, we need to ensure that whether you work in physical, personnel, information, or program security, we collaborate among ourselves and ensure that every functional discipline can share their recommendations about the complex problems we encounter. At AFS, we value contributions from across the entire organization. Whether you are a new personnel security processor, a physical security officer, provide staff support, or are a subject matter expert in the IT security field, you are a valued team member. We all work toward the same goal of providing the best security product to our clientele.

Senior leadership action
Our CEO, Board of Managers, and leadership team set the tone for security across our company. During my years in the federal government and private sector, I have been fortunate to work for many senior leaders who valued the input provided by career security professionals. Leadership's commitment requires involvement. As we know, employees are continually observing their leader's behavior and therefore it is imperative that leadership "walk the talk". We are very fortunate at AFS that our leadership recognizes security's criticality to our overall mission to protect our people, information, facilities, and assets, and our obligation to protect our clients' data and property. Leadership sets the tone by adequately resourcing our security discipline, integrating security into all aspects of our operations, and welcoming our participation at senior board meetings, business and proposal development opportunities, and senior strategy sessions.

Understanding the threat
The security landscape has changed over the years and security programs need to adapt. As a result, we utilize risk-management principles when providing security countermeasures. For example, the sophistication of our adversaries in the cyber area has become the principal threat facing our programs. No longer are we solely concerned with the physical removal of documents. Security programs require the right experience, tools, and resources to deal with

ever-changing cyber threats. At AFS, our leadership understands this reality and ensures that we have the resources to deal with complex threats.

Security training and awareness

Security training and educating our employees is very important. Based on personal experience, employees want to do the right thing and awareness is critical to the overall success of security programs. At AFS, we recognize the importance of continuous awareness when it comes to security. Our job is to both educate our employees and ensure that the messages are being received at all levels in the organization. We want employees to not only take the training, but to understand the rationale for the security requirements and put "Security First" when performing their duties. We aim to be approachable and available for our colleagues across AFS. To accomplish this, security is integrated into AFS programs as early as possible and we make ourselves available to provide assistance as needed.

Partnership with DSS

Whether in the federal government or in private industry, we are all working toward the same goal of protecting our national security. We worked very closely with our professional colleagues at DSS this year as they progressed on their journey of DSS in Transition. AFS served as one of the initial pilots in developing a Tailored Security Plan, which focused on transitioning security programs from compliance to a risk-management approach, and analyzing current threats to government assets. We appreciated the support and guidance we received from DSS across many of their functional areas. Building a true partnership with our DSS colleagues was critical to our success.

In summary, AFS is most appreciative of the Cogswell Award recognition we received; however, we will not rest on our accomplishments, as successful security programs must continually monitor themselves and strive for improvement.

Accenture Federal Services is a wholly owned subsidiary of Accenture LLP. It is a U.S. company with offices in Arlington, Virginia. AFS's federal business has served every cabinet-level department and 30 of the largest federal organizations. AFS transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations.

Espey Mfg. & Electronics Corporation

by Peg Murphy
Director Human Resources/Corporate Secretary/ Facility Security Officer
Espey Mfg. & Electronics Corporation, Saratoga Springs, N.Y.

Espey Mfg. & Electronics Corporation designs, develops, tests and manufactures specialized military and rugged industrial power supplies and transformers for use in harsh or severe environment applications. Espey is a small business certified by the Small Business Administration. Espey is an Original Equipment Manufacturing (OEM) company. Espey has been designing and developing "Best in Class" products in support of our government and the warfighter for more than 90 years.

I have worked on Espey's security team for nearly 40 years, 20 as the facility security officer (FSO). There have been many changes and challenges during this time. However, there has always been a constant commitment by those around me to secure and protect the critical technology that keeps the United States as the most powerful nation of the world. Since Espey is a small business and we all have multiple responsibilities, I recognize and support my team's passion in their continued efforts toward maintaining Espey's security program.

Our continued success is attributed to our senior leadership's commitment to security, a strong security team, continued education and training, outreach to customers and other FSOs, and to our strong partnership with DSS.

Senior leadership commitment and communication

Espey's CEO has established the guiding exclusive principle called C.A.R.E. – Customer Advocacy and Reliable Execution. This senior leadership commitment to Espey's security program is shared with the Program Management Office, its program managers, and all the active leaders in the company.

As a member of the senior leadership team, I can attest that this principle is communicated regularly and is fully endorsed and applies to everything we do. The Espey team has always taken pride in their strong commitment to the warfighter to develop, produce, and protect advanced power solutions that are used in critical military systems.

This message of commitment is communicated throughout the Espey facility from administration to the shop floor through regular announcements, brochures, all-hands meetings, posters, and required training.

Security team

The Espey security team continues to grow. I recognize certain seasoned employees, some who have served since the late 1980s and are still very active in the team's success. This includes Assistant FSOs George Sloan, Christine Earls and most recently Arthur Schrum. The last few decades, since the advent of email and the internet, our information security program would not be as robust without the expertise of Espey's Information System Security Manager (ISSM) and Information Technology Director Christopher Smith, along with the Information System Security Officer Allen Tucker.

Espey's ISSM's proficiency and knowledge on counterintelligence awareness, protecting against elicitation/recruitment attempts, and identifying our vulnerabilities have a huge impact on protecting all the information whether it's classified, unclassified or intellectual property. In addition, the team works diligently to report any cyber exploitation, hacking attempts or suspicious activities to the intelligence community.

Through the years, the Espey security team's passion has been focused on maintaining the highest standards for security, acting above and beyond what is described in the National Industrial Security

Program Operating Manual. The team is always applying rigor to improve its security posture. Most recently the focus has been on risk management, insider threat, re-definition of Espey's assets, and the latest security-related Defense Federal Acquisition Regulation Supplement guidance.

Security education and training
The security team's continual method of education and training includes the engagement of the entire workforce at every level. This regular and relevant education helps everyone understand and embrace Espey's stong security principles. The message always centers back to one team committed to protecting our critical technology. It has been noted that the passion and patriotism embodied by the workforce attests to the success of Espey's security training program.

Outreach
Espey's relationship with its customers goes beyond contractual obligations. It is extremely important as a custom design manufacturer to completely engage and understand the customer and end-use security requirements. The relationship engagement ensures that Espey not only meets contractual requirements but exceeds customer expectations. This is especially true in the development of drawings and test procedures on critical technology.

The security team understands that there is always more to learn. Collaboration with user groups, and other FSOs is fundamental to the success of the team. These relationships and events allow the team to give and receive feedback, continuously look for improvements, provide assistance or guidance as needed and share lessons learned.

Partnership with the Defense Security Service
Representatives of the Defense Security Service have always been members of Espey's security team. The relationship between DSS and Espey is foundational and it is the center of a strong security program. Many of Espey's security educational and training materials originate at DSS. We have seen several representatives throughout our history and have always been very fortunate in the professionalism, dedication, and willingness to help exhibited by the representatives assigned to our area.

In closing
I am very humbled that Espey Mfg. & Electronics Corporation is among the 39 facilities which were chosen from a population of approximately 13,000 cleared facilities. I accept this Outstanding Industrial Security Achievement Award representing Espey's security team and active leadership in honor of Colonel James S. Cogswell.

During a recent DSS audit at Espey, a DoD representative mentioned that, "Espey is a small company but swings a big bat to protect national security." This is Espey's third Cogswell award and we pledge to continue to practice the C.A.R.E. principle with extreme rigor toward the protection of critical technology.

Leidos

by Marcus Carpenter
Security Program Manager
Leidos, Reston, Va.

Leidos is a Fortune 500® information technology, engineering, and science solutions and services leader, headquartered in Reston, Va., that works to solve the world's toughest challenges in the defense, intelligence, homeland security, civil, and health markets. The company's 31,000 employees support vital missions for government and commercial customers worldwide. We are very proud of our Reston home office security team winning the Cogswell award, which we view as a testament to our company's focus on excellence and delivering uncompromised quality in every aspect of what we do.

The 2018 Cogswell award was especially gratifying as it covered a period of time when our work with our DSS partners was never more important. Due to our merger in 2017 with the Lockheed Martin Information Systems and Global Solutions business line, Leidos doubled in size overnight. This meant adding more than 16,000 employees and thousands of personnel clearances, hundreds of contracts and classified contracts, dozens of CAGE codes and locations, and additional inventory, while also integrating two different cultures to ensure a smooth transition to steady state operations.

If not for the strong partnership and extraordinary effort between DSS and our company during the merger, we may not have been able to sustain the superior level required to earn the Cogswell Award. Among others, DSS personnel such as Robin Nickel, Keith Minard, Sarah Beauregard, James Garrett, Patrick Fields, David Scott, Michael Halter, and Justin Walsh were instrumental in seeing us through this successfully.

We reached out to DSS early and often during this process and, as a result, DSS was able to understand the complexity of our challenges and provide guidance and support, thereby avoiding disruption of service to our customers both during and after the integration of the two companies.

Through the dedicated efforts of DSS personnel working with our security professionals, all aspects of the security requirements for the merger were successfully managed from the Cogswell-winning home office in Reston and operationalized across the company.

But our work with DSS is not limited solely to internal Leidos needs. For the past two years, Leidos has been a part of the DSS' Partnership with Cleared Industry program. The effort is a collaboration between DSS and 14 cleared industry partners sharing counterintelligence threat data. We meet weekly with our DSS counterparts in a secure environment to exchange information on these threats and discuss mitigation strategies.

Our Leidos security team has also been a part of the DSS Effectiveness Table Top Exercises in 2017 and 2018. In these exercises, a select group of leading defense contractors, including Leidos, worked together with DSS to develop best practices for insider threat programs. We continue to work with DSS to resolve challenges with insider threat reporting as well as exploring information-sharing obstacles. In time, the information gathered during these exercises may shape policy and define how insider threat program effectiveness will be measured.

Leidos' ability to establish such a close and collaborative relationship with DSS may stem, in part, from the fact that within the past five years, Leidos has hired nearly 5,000 veterans of the U.S. Armed Forces and that one in five Leidos employees is a veteran. Veterans know the importance of teamwork, and Leidos was recognized as one of Military Times' "Best for Vets" employers for the past five consecutive years (2014-2018). But Leidos' culture of teamwork and collaboration goes beyond our close ties to the military. We were named one of Fortune's 2017 Best Employers for Diversity, Forbes' America's Best Employers and Top 100 Corporate Citizens, as well as Ethisphere's 2017 World's Most Ethical Companies.

Leidos' team in Reston is complemented by corporate security professionals around the country and internationally who recognize the importance of achieving or exceeding all National Industrial Security Program Operating Manual, National Institute of Standards and Technology, Defense Federal Acquisition Regulation Supplement, and other compliance requirements. Leidos has been using a risk-based approach, much like DSS in Transition, to deliver uncompromised services and solutions to customer requirements at maximum value.

Leidos uses a centralized process for managing personnel security clearances required to support our customers via our Security Service Center (SSC). This facility is key to administering cleared personnel actions in conjunction with the facility security officer/ security managers, employees, program managers and recruiters. By moving routine administrative functions related to personnel security to the SSC, Leidos FSO/security managers can focus more attention on the local security program management and program protection. This process unites the management of our local security program in Reston with all others for more consistent program execution, proactive risk management, and better customer support.

Similar to the work performed at the SSC, Leidos also leverages a centralized model to efficiently and effectively administer its insider threat and counterintelligence programs. The Reston security team collaborates with corporate security resources worldwide both in detecting insider threat and counterintelligence risks, but also in mitigating, managing, and reporting with all required constituencies.

The collaborative nature of our security program has information security, insider threat, personnel security, regional security directors, and facility security officers working in lock-step with our DSS counterparts to provide a one team approach for security services.

The Leidos SSC delivers accurate, cost-effective, timely services using advanced workflow tools to ensure new employees are ready on day one to work customer programs. The Reston team receives weekly reports that outline any required upcoming actions related to anticipated terminations, periodic reinvestigations, and annual training requirements.

Additionally, Leidos deployed Arena ITI, a big data analytics platform, to assist its Insider Risk Management Program (IRMP). Leidos established its IRMP in 2014 and its team members work tirelessly to monitor employee activity and identify potential risk indicators related to intellectual property theft, sabotage, fraud, espionage, workplace violence and other threats. The IRMP team monitors all Leidos employees throughout the lifecycle of their employment and attempts to detect, deter, and mitigate insider risks, whether intentional (malicious) or unintentional (negligent), while protecting employees' privacy and civil liberties. The team uses Arena ITI to collect, analyze, and correlate vast amounts of data from numerous sources in a search for potential risk indicators. The team then scores and triages the risk indicators Arena ITI identifies in order to identify individuals who may present a higher risk to the company. A broader team then works to monitor and mitigate identified risks.

The Reston security team has also worked very closely with DSS in developing training programs that meet rigorous compliance and risk requirements. Interactive training materials for insider threat, annual refresher, derivative classification, etc., are typically reviewed with DSS before being implemented on the corporate learning platform, which provides easy curriculum delivery and centralized compliance tracking.

Similarly, security awareness and employee engagement initiatives like the "Mind Our Business" campaign are developed by the Reston team and shared across the entire enterprise. Guest speakers are invited from DSS and the FBI regularly to the Reston headquarters to keep employees up to date on current counterintelligence threats and security risks.

The Leidos security team is extremely proud of the relationship we have built with DSS as we strive for continuous improvement in our security approaches. We look forward to many more years of providing excellent security for our nation's classified information and excellent service to our defense and intelligence community customers.

Teledyne Scientific & Imaging

by Dorothy (Dotti) S. Bitner
Facility Security Officer
Teledyne Scientific & Imaging, LLC,
Thousand Oaks, Calif.

Teledyne Scientific & Imaging is comprised of Teledyne Scientific Company and Teledyne Imaging Sensors, which includes Teledyne Judson Technologies.

As Teledyne's Central Research Laboratory, Teledyne Scientific Company transitions technologies developed with contract research and development (R&D) investments from U.S. government R&D funding agencies into various Teledyne businesses. We are a technology leader in high performance compound semiconductor devices and integrated circuits, ceramic and functional materials, efficient real-time information processing algorithms, and optical sensors and assemblies.

Teledyne Imaging Sensors is a leader in high performance imaging systems for military, space, astronomy, and commercial applications. Our products include infrared (IR) and visible sensors, Read-Out Integrated Circuits (ROICs), IR scientific and tactical cameras, camera electronics embedded with advanced algorithms, and laser eye and sensor protection devices and filters.

Operating to the highest standards
Teledyne Scientific & Imaging, LLC conducts its business in compliance with the laws of the United States and other jurisdictions in which it operates and according to the highest ethical standards. Integrity is the cornerstone of the way Teledyne Scientific & Imaging does business. Ethical conduct is not only the right thing to do, it is good business.

Our security program is built on these principles, management support and an excellent partnership with DSS. As the facility security officer (FSO) I was honored to accept the James S. Cogswell Award on behalf of the management staff and employees who made this possible.

I cannot stress enough the importance of our partnership with the Defense Security Service. Whenever called upon, our DSS representative is always there to provide expert guidance and support. Being able to achieve the level of success needed to achieve Superior ratings cannot be done alone. Having a great security program, and a great working relationship with our DSS representative allows us to openly communicate and seek guidance on policy interpretations and in some cases, just have someone to confirm that you are "going down the right path."

In addition, we have formed great partnerships with the FBI and other government agencies to provide training to our employees through on-site presentation and participation in various other forums.

There are many aspects that go into building and maintaining a successful security program. The security staff does not do it alone. We rely on strong management support, dedicated employees, our great partnership with DSS, self-inspections, security awareness and continual education of our employees.

Education a key component
Educating our employees is a key component to the success of our security program. All cleared employees are required to complete an Annual Refresher Briefing and an annual Insider Threat Awareness Refresher Briefing. We have met this

"We rely on strong management support, dedicated employees, our great partnership with DSS, self-inspections, security awareness and continual education of our employees."

requirement with 100 percent completion. In addition to refresher training, we publish a quarterly newsletter that is sent out to all employees covering various topics such as espionage cases, reporting responsibilities, cyber security and insider threat, just to name a few. We developed a briefing for employees required to travel abroad for business or pleasure. The briefing is conducted prior to travel and upon return from travel. Current threat information is provided before they depart and the post travel debriefing is used to report any suspicious contacts and/or situations that may have occurred. The security staff partners with our information technology (IT) staff to sponsor an annual IT Security Awareness Fair.

In addition to training employees, the FSO must keep current with the training opportunities available through the Center for Development of Security Excellence and training seminars such as NCMS to ensure continued compliance with the National Industrial Security Program Operating Manual. The DSS website also has a wealth of information for the FSO to use in keeping the security awareness and training program, within the facility, current and relevant.

Achieving the Superior ratings and receiving the Cogswell award validate that the dedication and hard work that are put into creating and maintaining a security program are totally worth it.

University of Alabama

by Denise K. Spiller
Security Administrator
The University of Alabama in Huntsville, Huntsville, Ala.

In November 1949, Huntsville's leaders learned that their lengthy campaign to open a **University of Alabama** extension center in the city had been university approved. Both houses of the Alabama Legislature passed the bill, which enabled Huntsville and Madison County to purchase an additional 200 acres of land to build a proposed Research Institute. Spragins Hall and Madison Hall followed in quick succession, earning the center a promotion to "branch campus." But it wasn't until 1969, with the addition of Wilson Hall, University Center, and the Louis Salmon Library, that the University of Alabama in Huntsville (UAH) was made an autonomous university by The Board of Trustees of the University of Alabama.

Today, UAH is one of the nation's premier research universities, offering a challenging hands-on curriculum that ensures our graduates are prepared to become tomorrow's leaders. UAH is a public Tier 1 national university located in Huntsville, Ala., which *Southern Living* recently named one of the best college towns in the South. Its students hail from almost all 50 U.S. states and more than 80 countries.

The success of The University of Alabama in Huntsville is a combination of many elements, including guidance and support from the Defense Security Service, management support, employee participation in the security program, education and training support, and good relations with Government partners.

Guidance and support from DSS

DSS is a support system for the UAH security program. Our DSS representatives and the counterintelligence (CI) special agents provide students, faculty, and staff with training and expert guidance. Our DSS representatives have given feedback and suggestions during our annual assessment and throughout the year to enhance our program. They guide UAH to avoid any missteps that pertain to the program.

Management support

Senior management have led by example when it comes to participation in the UAH security training and their dedication to the program. They also provide support and the resources needed for the effective management of our program. They are unsatisfied with reaching the minimum requirement of security and strive to execute a higher performance.

Employee participation in the security program

Without our employees' participation, our security program would be severely lacking the means to be awarded a Superior rating during an assessment. They are very conscious of their reporting responsibilities. UAH has been recognized as one of the top reporters of suspicious contacts in the Southeast Region.

Education and training

UAH offers several training sessions throughout the year with a variety of topics including export control, cyber security, insider threat, and general security practices. Education is an ongoing process. By offering a variety of training dates, employees can attend an "in-person session" annually, which gives them immediate feedback to any questions or concerns they may have.

In-person training allows the employees to reacquaint face to face with the security staff, so we become approachable for reporting situations. UAH provides lunch and refreshments to both encourage and reward them for their support in attendance. UAH security staff try to use a variety of ways to promote security education, including newsletters, useful resources on our website, handing out doughnuts, and checking in on the students, faculty, and staff from time to time.

Relations with government partners

We have a great relationship with DSS and find having relationships with other government partners

a valuable resource. Some of these partners are the FBI, NASA counterintelligence special agents, and the Bureau of Industry and Security at the Commerce Department. Their expertise is essential to creating a strong security program and export control compliance. They are a resource that we use to provide security and export control training to our students, faculty, and staff.

By promoting security awareness throughout the university, the UAH security staff creates an atmosphere in which we are all working toward the same goal – to keep the warfighter safe and protect national security. It is a great honor to have received the Cogswell Award. It inspires us to continue going above and beyond the requirements of the National Industrial Security Program Operating Manual because that effort, in turn, is recognized by DSS. We congratulate and applaud all the Cogswell Award winners for this year and past years.

WorldWide

by Linda Richardson
Facility Security Officer
WorldWide Language Resources, Fayetteville, NC

WorldWide was founded in 1995 with a mission to deliver language training and operational linguist services to U.S. Special Operations forces. Over the past two decades we have grown into a leading international organization supporting commercial and government organizations in over 50 countries. Offering comprehensive, flexible and responsive language, auxiliary and logistics and manpower augmentation services, WorldWide is committed to providing the highest level of security possible to protect our employees and customers. We are grateful to be recognized for our commitment to security with the James S. Cogswell Award.

Prior to coming on board as the facility security officer (FSO) in 2013, WorldWide had received Unsatisfactory ratings on their two previous assessments. With that knowledge, I knew a significant amount of effort and dedication was going to be required to get the security program where I wanted it to be. After reviewing and overhauling the entire program, WorldWide received a Satisfactory rating on our first assessment, and after continuing to make improvements and refine our processes we received Superior ratings on our next three assessments.

This couldn't have been accomplished without a lot of hard work and dedication by my security team. We all worked long hours and put our hearts into our program ensuring that security and the company did the right thing every time. WorldWide's executive leadership was instrumental in ensuring that the Security Department had all the support needed to meet the organization's commitment to making our program a success.

I focused on several key areas that first year and then continued to build on those areas over the course of the following years.

Go back to the basics

I started out by reviewing the previous assessment vulnerabilities, and implemented processes and procedures to eliminate these from reoccurring. I also had to ensure that my team was properly trained; I wanted them to not only understand how to do something, but I wanted them to understand why they were doing it.

Self-inspections

These were crucial to identifying additional areas that needed attention and improvement. We also began completing employee interviews during our self-inspections with not only our corporate employees but more importantly with our employees located outside the continental United States. These interviews were instrumental to finding areas to improve and more importantly, identified vulnerabilities that we weren't aware of.

Security education

This was one of the areas that needed the most attention. We paid particular attention when completing initial security briefings with new employees ensuring they received a detailed briefing and encouraging direct communication with security. As a result of this, our self-reporting significantly improved. To go along with this we began notifying our employees directly regarding clearance determination actions required for final clearance determinations. As a result of both of these initiatives, our employees began to "own" responsibility for their clearance and all that this entails.

Adverse information reporting

This is the area where the most significant changes were made to our security program. Education and reinforcement for management and supervisors was the key to timely reporting to security. We now have a very robust reporting program and we always reinforce that it is our job to report and it is the government's job to adjudicate that reporting.

DSS as partners
In my first year and all of the following years, my DSS industrial security representative and counterintelligence special agent were instrumental to our success. They were always quick to respond to my questions, and provided me with recommendations and advice that proved invaluable. They cheered us on and always wanted us to succeed, and I cannot thank them enough for all of their support!

Don't be afraid to tell management 'No'
It's never easy to do this but it is your responsibility as an FSO to do this if you are asked to do something in violation of the National Industrial Security Program Operating Manual (NISPOM). Many times management doesn't understand all of the intricacies that we do so you may be able to recommend an alternate plan that is in compliance with the NISPOM.

Go the extra mile
Go out of your way to help your employees with their security clearance issues and questions. Make that phone call and ask what can be done to resolve that Loss of Jurisdiction that you didn't expect. We also always let our employees know that we are glad to review their DoD Consolidated Adjudications Facility/ Defense Office of Hearings and Appeals Statements of Reason responses. This has paid off in huge dividends for our company and many great employees have been retained by these efforts.

Actively work toward National Industrial Security Program (NISP) enhancements
Most NISP enhancements must be planned in advance and implemented throughout the year. Pick one, a few, or all that apply to your facility and research what you can do to qualify for those enhancements. Make a plan and set aside time on a regular basis to work towards those enhancements. You are already working hard at your program and this is the place where you can take credit for that hard work and your security program will be that much better for your efforts.

Mentoring and community support
Be there to support your fellow security professionals. WorldWide started this by providing free e-Fingerprint support to several companies. It quickly developed into an information sharing group. We all share

security news and policy updates, and we've come to rely on each other to bounce ideas off of and answer questions. I've also assisted other companies with their self-inspections, and by stepping out of the comfort zone of my company's program, I've learned so much more which has helped me further improve our program.

These are the building blocks that I used to make my program better and made our James S. Cogswell Award possible. Think of your security program as those building blocks. Build your program until you have a strong base; once that is in place, keep adding blocks as you make improvements and enhancements, and before you know it you will have a fortress. This fortress will protect your company, your employees, your clients and ultimately our nation.

DSS employees receive awards at NCMS TRAINING SEMINAR

by Beth Alber
DSS Public Affairs

During this year's annual NCMS training seminar, several DSS employees were presented with Industrial Security Awards:

The Albuquerque Resident Office was recognized for working diligently to improve security procedures, practices and policies through the development of a strong partnership between industry and government.

The Atlanta Field Office was recognized for being a tremendous partner whose synergistic mission, vision and goals were instrumental in serving the professional development of NCMS Georgia Chapter members.

Lisa Gearhart, formerly with Industrial Security Integration and Application Directorate and now with the Defense Vetting Directorate, received the award for her work on the National Industrial Security Program Contracts Classification System (NCCS).

The Purple Arrow program was recognized for materially and beneficially affecting the security community by providing support through a team of counterintelligence professionals from multiple agencies who have dedicated themselves to protecting classified and sensitive technology throughout New Mexico. DSS team members were Nick Luce, counterintelligence special agent from the Phoenix Field Office, and former DSS employee Paul Godlewski.

The Industrial Security Award is presented to an individual or organization that has significantly contributed to industrial security and meets a minimum of two of the following criteria:

- Individual or organization that has materially and beneficially affected the security;
- Individual or organizational contribution which improves security procedures, practices or policies of national interest (i.e., develop partnerships between industry and government, involvement in ISACs, industry teams, etc.);
- Individual or organization continuing contributions to the Society by enhancing the mission, vision, and goals of the Society;
- A member or associate member in good standing.

Albuquerque Resident Office
The DSS Albuquerque Resident Office — Industrial Security Representatives Patricia Bourgoyne and Juan Carrillo, and former DSS employee Counterintelligence (CI) Special Agent Paul Godlewski — routinely attends and speaks at the NCMS Enchantment Chapter meetings, ensuring they are an integral part of the local security community. The community benefits from their experience, and their willingness to provide training and support to the entire community. During the past year, they provided several training opportunities for the local community.

Industrial Security Representative Juan Carrillo (left), Albuquerque Resident Office, stands with DSS Director Dan Payne. (Photos courtesy of NCMS)

Godlewski developed a close and productive relationship with cleared companies in the New Mexico region, and as a result, the total number of suspicious reports received from industry in the Albuquerque area is now the seventh highest in the nation and fourth highest in the Western Region.

He made himself available to provide CI presentations throughout the region of responsibility, including traveling with Carrillo to New Mexico State University, where he was invited by the chancellor to provide a DSS overview and briefing on the threats to academia to the Office of the Presidents and the university's deans.

Atlanta Field Office
The DSS Atlanta Field Office — Field Office Chief

Kelly Grace, Information System Security Professional Renee Lumpkin, Industrial Security Representative Mark Minar, and CI Special Agent Justin Shanken — has been instrumental in increasing the industrial security and counterintelligence training and awareness of the NCMS Georgia Chapter 16 and its members. DSS Atlanta helped to organize and coordinate subject matter experts in support of two annually recurring security seminars, now in their seventh year of success. Guest speakers have included representatives of Department of Energy, FBI, Department of State, DSS and many others.

Grace partners with the Georgia Chapter to schedule and conduct a recurring quarterly 'Coffee with the Chief' roundtable. This rotating informal meeting provides a personal and open dialogue between the field office chief and company representatives to address challenges, concerns or questions; in return, she gets direct feedback on the industrial security needs in the Atlanta Field Office area of operations.

Jane Dinkel (left), NCMS Awards Committee and Lockheed Martin Missiles & Fire Control, stands with members of the Atlanta Field Office (from left) Industrial Security Representative Mark Minar, Information System Security Professional Renee Lumpkin, and CI Special Agent Justin Shanken.

Lisa Gearhart

From 2015 to 2018, Gearhart served as the program manager and functional lead for the National Industrial Security Program Contracts Classification System (NCCS), a system designed to streamline the DD254 for industry and DoD. During this time, she was responsible for ensuring NCCS implementation within DoD, 32 Federal agencies that have signed agreements with DoD for NISP oversight, and over 13,000 cleared companies. She served as the single point of contact for the system and worked with customers to spread awareness and gather requirements.

Lisa Gearhart (left), Defense Vetting Directorate, stands with DSS Director Dan Payne.

Gearhart developed a partnership with NCMS to develop and provide training and educational materials. She held four two-day workshops for selected NCMS members to attend and beta test the system in order to improve functionality. She worked with industry to ensure that users were engaged, to identify gaps, and to mitigate issues. She also provided three brown bag training sessions for members and provided training to over 14 NCMS chapters.

Purple Arrow program

Created in 2008, this group was initially called the New Mexico Counterintelligence Working Group, but was renamed Purple Arrow in 2014. The group includes representatives from DSS, FBI, Department of Homeland Security, and Defense Threat Reduction Agency. Not long after forming, members immediately reached out to the defense industry in an effort to learn how they might best support security professionals in the region. Among those spearheading the efforts were CI Special Agent Nick Luce and former employee Paul Godlewski, who replaced Luce in 2014. The group created a daily newsletter that includes current news events relating to insider threat, espionage, cyber security, and other similar topics, and is distributed to over 7,000 recipients. In addition to the daily newsletter, Purple Arrow distributes real-time threat warnings to the community as they arise.

Purple Arrow continues to support the NCMS Enchantment Chapter and local cleared defense contractors by regularly attending and presenting at NCMS Enchantment Chapter meetings. As a group, they share relevant topics with members and address questions and concerns attendees may have. Because of the enhanced communication between the industrial security community and Purple Arrow, and their willingness to share results, the awareness of the importance and significance of suspicious contact reports has greatly increased, resulting in a substantial increase in the number of reports submitted.

22ND ANNUAL FOCI CONFERENCE: Developing a DSS playbook for staging victory in industrial security

by David L. Brem and Luke A. Haugen
Industrial Security Integration and Application

"We must secure the 'home game' and rise to the challenge of the 'away game'," said Fred W. Gortler, director of Industrial Security Integration and Application (ISIA), during the 22nd annual Foreign Ownership, Control, or Influence (FOCI) Conference, held in June at the U.S. Patent and Trademark Office in Alexandria, Va.

Gortler's theme echoed with the 546 conference attendees: The United States is losing the industrial security battle. But by strengthening FOCI policies and partnerships with the U.S. cleared industrial base, U.S. national security will be fortified.

During his comments, the Honorable Joseph D. Kernan, Under Secretary of Defense for Intelligence (USD(I)), noted the significant threat posed by foreign adversaries and how the partnership between DSS and industry is vital to safeguarding national security. Kernan applauded the DSS move to a tailored, risk-based methodology from a checklist, compliance-based approach.

DSS Director Daniel Payne detailed why the switch to a risk-based methodology is paramount. "Basic level security isn't good enough…seeing how you are protected and how your adversaries are coming at you shows what is being exploited," he said. He noted that knowing this information allows for a threat-driven, risk-informed approach to industrial security.

The various sessions at the conference detailed the risk-based methodology and its impact on industry.

The "Executive/Legislative Reform" panel began with a discussion on the paradigm shift in industrial security. Moderated by Keith Minard, assistant director for NISP Administration and Policy Analysis,

During the 'Navigating Risk-Based Engagements' panel, members discussed mitigating risk and included (from left to right) John Massey and Andrew Winters, Industrial Security Field Operations; and Stanley J. Borgia, vice president of Corporate Security, Rolls-Royce North America Holdings, Inc.

the panel commended the administration's commitment to issuing new policy guidelines that strengthen internal and external security oversight measures, enabling industry to better identify corporate threats. Proactive mitigation strategies will enable FOCI companies and directors to better detect, repel, and defeat adversarial threats.

The "Navigating Risk-Based Engagements" panel discussed the future of DSS, including guidelines on how to identify assets, understand threats to those assets, and effectively protect the assets. The panel explained how the 12x13 charts help identify the methods of operation and methods of contact industry may encounter to assist with mitigating the risks.

The "Delivering Uncompromised" panel discussed the need to encourage dialogue and action between government and industry to ensure victory over its adversaries and competitors. The burden is on the entire government and industry to protect and safeguard classified information.

The Outside Director/Proxy Holder (OD/PH) Reform panel, moderated by Dr. David P. Grogan, deputy director, ISIA, covered the reform, which embodies DSS' new risk-based approach by harmonizing the OD/PH fiduciary and national security roles into one succinct package. Guidelines include new and updated processes for the nomination, training, and evaluation of OD/PH and the FOCI board. The new approach will increase expectations for board room performance and aid companies in creating a high performance board.

During the OD/PH Cyber Panel, moderator Dr. Samantha Ravich, chairwoman of the board, Foundation for Defense of Democracies' Transformative Cyber Innovation Lab, discussed a case study that underscores the importance of maintaining a strong cyber infrastructure. Ultimately, it is imperative to understand the role of the board, ensuring the company is investing in the right assets, abiding by the right policies, and is doing so the right way.

The FSO Cyber Panel elaborated on the important steps of cyber risk mitigation for industry, beginning with risk identification. Following risk identification, plans for threat mitigation begin. Karl Hellmann, DSS NISP Authorization Office, stated these plans are "the U.S. cleared entities responsibility to make sure the controls are being implemented, not the foreign parents."

TOP: Gloria Sutton, facility security officer with Airbus Defense & Space, Inc., networks during one of the conference breaks. **BOTTOM:** Karl Hellmann (left), Industrial Security Field Operations, discusses the importance of cyber risk mitigation for industry. (Photos by Hollie Rawl, CDSE)

The National Interest Determinations (NID) panel members stressed the importance of submitting a complete and accurate package, which will result in a quicker process and determination. The panel addressed confusion and the FSOs left with a better understanding of NIDs.

The Insider Threat Update panel complimented the FSOs, noting their excellence in insider threat implementation, and provided information on resources to use for training, such as the Center for Development of Security Excellence.

A Q&A with **Cherry L. Wilcoxon**, Senior Advisor/Chief Financial Officer

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

Cherry L. Wilcoxon, a member of the Defense Intelligence Senior Level, is the Senior Advisor/Chief Financial Officer for DSS. As such, she is the principal advisor to the agency director in financial programming, budgeting, regulatory compliance, and other enterprise-wide financial matters. She directs the financial management activities of the DSS enterprise and provides leadership across the spectrum of agency operations, integrating support elements into the overall mission planning, budgeting, and execution. Prior to this appointment, Wilcoxon served as the deputy, Financial Management division and Comptroller, DSS.

She began her federal career in 1991 with the Department of the Air Force, as the Personal Financial Manager at the Bitburg Air Base Family Support Center, Germany. During her 20 years with the Air Force, Wilcoxon held a variety of positions with increasing responsibility, to include Personal Financial Manager, Resource Advisor, Instructor, Course Director, Budget Analyst, Budget Officer, and Director of Resource Management.

Q: Tell us about your background.

I think the most important thing to know about my background is that I have worked from the bottom up in the financial management field. I've worked in operations and as a policy maker. So I understand both sides and I don't just look at policy as a concept, but I look at how a policy will affect our operations. And along the way I have worked in a number of different DoD activities. This has given me a broad perspective of how the Department works.

Q: What led you to this position?

Honestly, the first thing that attracted me to the position was quality of life. I was working at the Defense Intelligence Agency and spending too many hours commuting. When this job opened up closer to my home, I jumped at it. However, what has kept me here is the constant challenge and opportunity to grow professionally. Since I have been at DSS, I have not had one uneventful year. Change has been a constant theme. For example, during my first year here we were operating under sequestration and shortly after I came on board, I had to sign my furlough notice. Since then, we have stood up the Defense Insider Threat Management and Analysis Center, dealt with headquarters delayering, and shortages in funding for personnel security investigation for industry.

Q: How has the Financial Management field changed since you came into federal service?

Financial Management in government has gone through massive change and evolution in how we manage public resources. Though the Planning, Programming, Budgeting and Execution model of the 1960s has remained intact, its application has tremendously evolved. The scope of expertise of Financial Management professionals can no longer be single focused. Finance professionals must be dynamic to remain relevant to the organizational mission, its resource requirements, and the needs of various internal and external stakeholders. We operate in a constantly changing environment, and we are constantly challenged to bridge and mitigate mission needs and gaps with resource requirements. I have been fortunate that in every job I have had, leadership has understood the importance of the financial management function and the interdependent relationship of how operational decisions affect resources and mission results. I can't protect, defend and advocate for resources unless

I am tied into the agency's operational decisions. Over the last 15 years, the Department has made two significant capital investments to develop the competencies of the FM workforce: Certified Financial Management Managers and the DoD FM Certification program. I think the certification programs have helped to move the field from being viewed as a pure bookkeeping function to a true financial management and analysis function. Another example is the Internal Controls Program where it previously focused almost exclusively on misuse of government credit cards or travel cards. Now, the program takes a broader view of agency activities and we leverage the program to inform decision makers.

Q: What do you see as the biggest challenge facing DSS from a Financial Management perspective?

Right now, our biggest challenge is establishing a Working Capital Fund (WCF) infrastructure to support the transfer of the background investigation mission from the Office of Personnel Management to DSS. We have to set up the infrastructure, develop a means to issue auditable and supportable invoices and collect payments, and ensure DSS WCF operations remain solvent at all times. In addition, we have to ensure it is operating efficiently to keep the cost of investigations stable.

I think another big challenge is the stability of the workforce. As we assume new missions, the financial management landscape will become increasingly complex. We need employees with both breadth and depth of experience, not only in financial management, but I would argue across the agency. We need people who are curious, who think outside the box and can thrive in a changing environment.

Q: The agency is looking at a number of new missions coming in the next year or so. How does that affect your staff and your job?

As I said, one of the biggest challenges right now is establishing a Working Capital Fund. I will be looking to hire people who not only understand the WCF business but are curious, thoughtful and deliberate in their actions. The new mission has energized FM and I see opportunities for professional development and growth. While at the same time, we have to continue to maintain our current operations and support the rest of the agency. It is imperative that FM remains creative and agile to meet the demands of an ever-evolving agency mission.

Q: Being able to conduct an audit of the Department of Defense has been a big push. What is the status of DSS and its audit readiness? What are the next steps?

As a defense agency, DSS is part of the Fourth Estate in the Department. Our annual operating budget is less than $1 billion. And since funding for personnel security investigations and civilian pay account for roughly 70 percent of our budget, we are not required to submit to a full financial statement audit. That said, we are sustaining audit readiness through our internal controls strategic plan. I recognize that the audit readiness program provides the checks and balances needed to ensure that we are operating with accountability and fiduciary responsibility to our greatest stakeholder; the American people. Once the vetting mission fully transfers and we establish the Working Capital Fund, we could be looking at a total program greater than $2 billion. At that time, I expect DSS will undergo a full financial statement audit.

Q: What advice or guidance would you give to the DSS workforce in terms of where the agency budget is going?

First and foremost, be receptive and open to change. Stay positive. I know there is a lot of uncertainty, but I think as a senior leader, my job is to keep my staff motivated and focused. I think one of the ways to do that is to be as open and transparent as possible with the changes in the environment.

In terms of the budget, the Secretary has stated that in fiscal year 2018, the Department received a large increase in overall funding. Future years will adhere to this new top line and we should not expect another increase. That means the Department and DSS will be evaluating reforms and efficiencies for cost avoidance or savings. For instance, we need to reduce redundancies and consolidate similar functions, especially at the headquarters levels. A good example is the move to enterprise email for the Department. So in short, as we take on new missions, we will see increased funding. At the same time, we will continue to experience budget tightening with the focus on reform and gaining efficiencies where we can.

OKLAHOMA CITY REMEMBRANCE

'The spirit of this city and this nation will not be defeated'

Editor's note: *The following is a first-hand account of a DSS employee who attended this year's Oklahoma City Remembrance Ceremony. The article reflects her thoughts and opinions.*

by Denise Arel
Office of the Chief Financial Officer

On April 19, 2018, Oklahoma City marked the 23rd anniversary of the bombing of the Alfred P. Murrah Federal Building. Each year, on the day of the bombing, Oklahoma City pauses for a remembrance ceremony to honor the 168 victims of the attack, along with their families, survivors, and those changed forever. DSS senior leaders have been in attendance since 2012, and this year, Troy Littles, DSS Executive Director, represented DSS.

Prior to the ceremony, hundreds of people gathered on site to remember the men, women, and children who were killed; some placed flowers on the remembrance chairs and some found seats along the Reflecting Pool to reflect and remember.

A group of bagpipers opened the ceremony by leading the procession of dignitaries, speakers, and survivors to the stage. While observing the procession, we were joined by a woman in a wheelchair who introduced herself as Daina Bradley, a survivor of the bombing. At the conclusion of the processional, Michael Turpen, chairman of the Oklahoma City National Memorial Foundation, provided introductory remarks.

At 9:02 a.m., the crowd paused for 168 seconds; one second for each life lost. Shortly after, Oklahoma City Mayor David Holt remarked on those whose lives were changed forever as a result of the bombing. Twenty-three years ago, he was a sophomore at Putnam City North High School when the bombing occurred.

"It is incumbent on my generation and rising generations, especially if we live here in Oklahoma City, to carry on the lessons of April 19," Holt said, "and to touch lives and make sure that all who experience this place are changed forever." He concluded by saying that as a young citizen of

TOP: The museum features several exhibits related to the Oklahoma City bombing. **BOTTOM:** The Oklahoma City National Memorial Museum is housed in the Journal Record Building, which was formerly the offices of The Journal Record newspaper.

The Survivor Tree was heavily damaged by the bomb, but has not only survived but thrived. It is surrounded by a short wall, on which is inscribed, "The spirit of this city and this nation will not be defeated; our deeply rooted faith sustains us."

Oklahoma City, he is committed to telling the story of the bombing.

Oklahoma Governor Mary Fallin addressed the crowd, stating that in 1995, her children were then 4 and 7 years old, and are now 27 and 31. While her children remember very little of that day, she wants future generations to never forget.

Following Governor Fallin, former Governor Frank Keating paid a special tribute to the late Reverend Billy Graham. Four days after the bombing in 1995, Graham visited Oklahoma City to hold a public prayer service. The former Governor quoted some of Graham's words from 1995 that are now etched around the Survivor Tree, "The spirit of this city and this nation will not be defeated; our deeply rooted faith sustains us." Six audio clips from Graham's sermon on faith and resiliency were played while local guitarist Cole Grubbs sang a selection of hymns.

The event concluded with the reading of the names of the 168 people who died in the attack. Melissa Canales, daughter of Kathy A. Finley from the Federal Employees Credit Union, read the names of the five Defense Investigative Service employees killed on the third floor of the Murrah Building — Robert G. Westberry, Larry L. Turner, Norma 'Jean' Johnson, Peter L. DeMaster, and Harley Richard Cottingham.

Following the ceremony, we visited the Field of Empty Chairs adorned with flowers and other items of remembrance where we received a warm welcome from the DeMaster, Johnson, and Turner family members who were in attendance.

As we toured the museum, we came across Daina Bradley's story, the woman who sat next to us during the remembrance ceremony. Before the bombing, Daina Bradley, with her two small children, her sister and her mother walked into the Social Security Office of the Murrah Building. After the blast, rescuers found Bradley's right leg pinned under a fallen concrete beam, but could not move the beam. To save her life, an orthopedic surgeon had to amputate Bradley's lower leg with his pocket knife. Bradley's two children and her mother were killed in the explosion, and her sister was severely injured. Reading about her story was emotionally overwhelming.

Attending the remembrance ceremony was truly a humbling experience. From the ceremony itself, to meeting the families and embracing Bradley, to every symbolic detail on the memorial grounds, visitors are left with a greater appreciation of what transpired that fateful April morning that will forever be memorialized in America's history.

Next generation training delivery platform enhances current system

The Center for Development of Security Excellence (CDSE) is scheduled to launch its next generation training delivery platform in October 2018. The new delivery platform retains the name STEPP (Security Training, Education, and Professionalization Portal), but features several enhancements, to include increased functionality, improved performance, and unlimited user capacity.

These enhancements are possible because STEPP will be hosted on the Office of Personnel Management's USALearning™ platform, which provides an open-source, cloud-based, and customizable solution for delivering security education, training, and awareness products and services. Moreover, the new STEPP training delivery platform includes a full array of learning technology plug-in options for meeting future requirements.

This new platform represents a major leap forward in achieving the CDSE goal of providing the DoD and other stakeholders with the security education, training, and awareness they need at the time, place, and on the approved devices of their choosing. It also forms the foundational component for the DSS Security Knowledge Management System (SKMS).

As envisioned, SKMS will be an integrated system of systems designed to increase collaboration across the security community, improve course development and management, and enhance the learner experience.

The need for security education, training, and awareness products and services has grown exponentially over the years. With the emergence of new, dynamic, and complex threats to U.S. national security, the increasing demand for these products and services from CDSE will continue to rise.

In addition, CDSE is poised to assume responsibility for designing, developing, and delivering training products and services for other mission areas to include controlled unclassified information, unauthorized disclosure, continuous evaluation, insider threat, and background investigations.

As an integrated system of systems, SKMS, with the new STEPP platform as the first system, will enable CDSE to scale to successfully meet this increased user and mission demand.

Focus of Operational Training Events to improve DiT understanding

by John B. Massey
Industrial Security Field Operations

More than 600 DSS employees recently received training at two Operational Training Events in San Diego, Calif., and Orlando, Fla. These events included personnel from Industrial Security Field Operations, Industrial Security Integration and Application, Counterintelligence, and DSS Headquarters. This year's training focused on the new "DSS in Transition" (DiT) methodology, which DSS began implementing in January 2018.

The training event provided DSS personnel with an understanding of the security baseline and foundational elements of a security review. It also enabled attendees to identify the content of a Plan of Action and Milestones (POA&M) and the components of a Tailored Security Plan (TSP). These four terms are associated with key steps in the new DiT methodology and the training of these concepts was essential to the success of the two events.

Attendees were reminded they would not become experts on the DIT methodology after completion of the training, but should have a solid foundational understanding of the new methodology in advance of their participation in a DiT phased implementation review before the end of 2018. Post-event surveys administered to attendees indicated that personnel felt much more comfortable in their understanding of the DiT methodology after the training.

In advance of the training, DSS personnel attending the event reviewed the "2017 Trend Analysis of Cleared Industry Reporting," Concept of Operations for a Tailored Security Program, and a Threat Assessment Report. After arriving, each attendee was provided with a training binder that contained copies of all content and presentations from the training. Personnel also attended training sessions on the following DiT-related topics:

- Security baseline: Asset identification and security controls
- Preparing for a security review
- Completion of the Tailored Security Plan

Each of these topics were presented by a cadre of personnel who supported the DSS Change Management Office in 2017, served on the DiT methodology development team, or participated in one of the four DiT reviews from the first phase of implementation. A practical exercise was conducted at the conclusion of each training block to ensure comprehension of the material. In advance of these sessions, personnel were provided an introduction to the technology of focus for DiT implementation and an overview of threats, sources, tools, and application of threat data.

During the four-day event, attendees also received instruction on human relations and leadership development and were provided briefings from the DSS Enterprise Mission Management Cell, Business Analysis Unit, Personnel Security Management Office for Industry, Operations Analysis Group, and Defense Insider Threat Management and Analysis Center. Instruction was also provided on handling, storing, and sharing classified information and information handling procedures.

Each of the two training events began with opening remarks from DSS senior leaders. DSS Director Dan Payne provided opening remarks at the San Diego Operational Training Event; and Deputy Director Jim Kren opened the Orlando session. These remarks provided a review of recent DSS activities and a glimpse into the future roles and missions of the agency. Members of the DSS workforce were also recognized with time and service awards and for the completion of internal training curriculums to include the National Industrial Security Program Oversight Course, Managing Risk through Industrial Security course, and Applying Industrial Security Concepts course. The events concluded with breakout sessions for each DSS directorate.

Empowering the next generation objective of mentoring conference

by Israel Seda-Sanchez
Human Capital Management Office

Mentoring provides an opportunity for employees to enhance their professional and personal networks, knowledge, and skills. With five agencies housed in the Russell-Knox Building, the DSS Human Capital Management Office (HCMO) realized there were potentially untapped mentoring opportunities that existed in the building. To encourage personnel to seek mentor/mentee relationships, possibly with people outside their home agency, HCMO recently hosted an Inter-Agency Mentoring Conference, with a theme of "Empowering the Next Generation."

La Shawn Kelley, chief, HCMO, opened the event and introduced the morning's keynote speaker, Kathy Wentworth Drahosz, president and CEO of The Training Connection, Inc. Drahosz discussed the importance of mentoring in developing a new generation of leaders, the differences between formal and informal mentoring, the mentoring process, and best practices of a successful mentoring program.

Immediately after, participants proceeded to one of three breakout sessions.

Raymond Campbell, director of DSS' Diversity and Equal Opportunity Office, discussed "The Benefits of Diversity in Mentoring," which included information about unconscious bias.

Dr. Fred Bolton, program manager, DSS Leadership Development Program, examined "The Importance of Mentoring in Leader Development." Participants in this session worked in groups to discuss the importance of mentoring when developing leaders, and provided their own perspectives and suggestions about real issues within their organizations.

Elnora Wright, Government-wide Mentoring Program manager at the Office of Personnel Management, facilitated "Cross-Generational Mentoring," an interactive discussion about the benefits, values, and challenges individuals from different generations face when paired together.

In the afternoon, several DSS senior leaders participated in a panel discussion, fielding questions and relating their mentoring experiences and how having a mentor affected their respective careers.

Later, Air Force Capt. Heather Novus, commander, Military Personnel Flight, Field Support Squadron, Air Force Office of Special Investigations, spoke about the importance of mentors throughout her military career, their impact on her as she faced "ups and downs," and what she has found to be mentoring best practices.

Kelley closed the conference by reiterating the benefits of mentoring as a career progression tool and asking the audience to consider the conference a "call to action" to establish and/or continue mentoring relationships, both within and outside of one's home agency.

TOP: Jeffrey Cavano, Industrial Security Integration and Application, participates in an exercise during a break-out session. **BOTTOM:** (From left) Donna Maxey, DSS Strategic Management Office, William Sofranko, Industrial Security Field Operations, and Don Carey, DSS Human Capital Management Office, work through a leadership development exercise.

DSS welcomes new senior leaders

PATRICIA P. STOKES, the director of the Defense Vetting Directorate, was recently promoted to the Defense Intelligence Senior Executive Service.

As the DVD director, she is responsible for the implementation of the transfer of the background investigation mission from the National Background Investigations Bureau to the Defense Security Service. She is responsible for overseeing the transition and positioning DSS to fully execute the mission for the Department of Defense.

Prior to joining DSS, she served as director of Security for the Department of the Army as the Senior Security Advisor in the Office of the Deputy Chief of Staff for Intelligence. She was instrumental in leading several Personnel Security Reform initiatives for DoD, and is recognized as a key DoD subject matter expert driving change and innovation for the DoD security enterprise.

Her federal service career began in 1980 and Stokes has worked exclusively in Security since 1987. She has held several senior security positions for the U.S. Army, U.S. Navy, U.S. Special Operations Command, Missile Defense Agency and DSS. She received the Presidential Rank Award of Distinguished Executive in 2015.

CHERRY L. WILCOXON, Senior Advisor/Chief Financial Officer, was recently promoted to the Defense Intelligence Senior Level.

In this capacity, Wilcoxon is the principal advisor to the director of DSS in financial programming, programming, budgeting, regulatory compliance, and other enterprise-wide financial matters. She directs the financial management activities of DSS enterprise and provides leadership across the spectrum of agency operations, integrating support elements into the overall mission planning, budgeting, and execution.

Prior to joining DSS, Wilcoxon served as the chief, Accounting Operations Division, for the Defense Intelligence Agency (DIA), responsible for providing agency-wide accounting operational support for the DIA mission. She began her career in 1991 with the Department of the Air Force, as the Personal Financial Manager at the Bitburg Air Base Family Support Center, Germany. During her 20 years with the Air Force, Wilcoxon held a variety of positions with increasing responsibility, to include Personal Financial Manager, Resource Advisor, Instructor, Course Director, Budget Analyst, Budget Officer, and Director of Resource Management. Most recently, Wilcoxon served as the deputy, Financial Management Division and Comptroller at DSS, before being named the Chief Financial Officer.

DR. DAVID P. GROGAN, deputy director of Industrial Security Integration and Application (ISIA), was recently promoted to Defense Intelligence Senior Level.

As the ISIA deputy director, Grogan works with internal and external stakeholders across government and industry to assess and mitigate risk to classified technology and information in the cleared industrial base.

Prior to joining DSS, he served as the director of Analysis at the National Ground Intelligence Center. He spent five years in the commercial sector leading companies and corporate divisions through periods of significant change, facilitating acquisitions and post-merger integration.

Grogan served over 20 years in the U.S. Army. During his military career, he spent time as an infantryman, intelligence officer, and Middle East Foreign Area Officer, and his assignments included nearly 12 years in Europe and the Middle East.

ANDREA LUQUE, the senior advisor for Operations (Personnel Security and Suitability) of the Defense Vetting Directorate, was recently promoted to Defense Intelligence Senior Level.

Luque has over 30 years of collective security and intelligence experience. She began her career in 1988 with the U.S. Army, as a Signals Intelligence Analyst, and started her civilian career in 2003. She has held key positions in the Security functional area, to include the Special Security Office, U.S. Army Intelligence and Security Command; command inspector for the Personnel and Industrial Security Program, Army Material Command; acting deputy director for Personnel Security, Office of the Under Secretary of Defense for Intelligence; functional manager (Security Budget portfolio) and later as the chief, Personnel Security, Headquarters Department of Army; and recently as the director, Army Personnel Security Investigation Center of Excellence.

Nammo Talley recognized for excellence in counterintelligence award

DSS Director Dan Payne recently recognized Nammo Talley Inc., for winning the 2017 DSS Excellence in Counterintelligence (CI) Award. Payne presented the award to Chad Parkhill, President, and Michelle Hart, manager for Regulatory Compliance and Facility Security Officer, Empowered Official, Nammo Talley Inc.

Nammo Talley Inc. develops, produces and tests propellants, explosives and energetic devices in support of the U.S. and allied defense forces. Products range from ejection seat rockets to lightweight man-portable shoulder-fired systems, and other munitions.

The DSS Excellence in CI award program was established by DSS CI Director William Stephens in 2010 to encourage and reward companies that strive to deter, detect, and disrupt the theft of sensitive or classified U.S. information and technology by foreign entities. The selection program is highly competitive and only a few cleared companies or institutions are selected annually. These companies' CI programs enhance national security and promote the uncompromised delivery of sensitive and classified services and capabilities to the Department of Defense and other U.S. departments and agencies.

During his remarks Payne acknowledged Nammo Talley Inc., for exceptional cooperation with DSS and the government, and for consistently producing the highest quality reports received by DSS CI from across cleared industry. Payne noted that Nammo Talley Inc. reporting led to the identification of subjects involved in terrorism; international black marketing in arms; and an arrest and charges against two individuals for Violation of the Arms Export Control Act and smuggling goods from the U.S. Payne also recognized Nammo Talley as a leader and mentor in national security within the community of its peers.

Parkhill, in his remarks, acknowledged and thanked the director and DSS. Parkhill highlighted the importance Nammo Talley Inc., places on counterintelligence, as well as the company's "very

strong and positive relationship with the Defense Security Service." Parkhill noted the relationship was "built on a core principle common to both DSS and Nammo Talley ... to protect the warfighter." Parkhill also thanked DSS CI Special Agent Jon Laahs, Western Region, for his support and partnership.

In addition to Nammo Talley Inc., The Texas A&M University System was also selected for the 2017 Excellence in CI Award from a field of six finalists. Payne also sent formal letters of recognition to chief operating officers of the other finalists: Auburn University, Astronics Test Systems, A-Tech dba Applied Technology Associates, and Carnegie Mellon University.

CDSE receives multiple awards in recognition of its efforts

by Aimee Stehman
Center for Development of Security Excellence

The Center for Development of Security Excellence (CDSE) continues to fulfill its mission of being the premier provider of security education, and was recently recognized for its efforts by several organizations.

For the third year in a row, CDSE's Curriculum Manager Rebecca Morgan was awarded the Counterintelligence Individual Award for CI Educator of the Year. This award is issued annually by the National Counterintelligence and Security Center.

The Defense Security Service received the *DITEB Award*, Gold Level of Achievement, for organizational performance and major accomplishments in support of the DoD Intelligence Training and Education Board (DITEB) vision, mission, and principles of interoperability, synchronicity, transparency, efficiency, and quality.

The *Omni Awards* are a nationally known competition that recognizes organizations for innovative work that empowers audiences. The awards committee is represented by multiple high profile companies, to include the Olympic Organization Committee, and multiple major media outlets. CDSE captured several awards for products developed by the Training Division and was recognized again this year.

Finally, the *Horizon Interactive Awards* is one of the most prestigious awards in the area of interactive and creative media. CDSE has received medals for products each year for the past 10 years.

Below are the courses and products that won Omni and Horizon Awards for 2018.

- **DoD Annual Security Awareness Refresher**
  Omni Award: Bronze, Educational Category; Bronze, Government Category. *Horizon Interactive Award: Bronze*.
  This eLearning course refreshes students' basic understanding of initial security training requirements outlined in DoDM 5200.01 Volume 3, Enclosure 5, National Industrial Security Program Operating Manual.

- **Technical Implementation of Assessment and Authorization in the NISP**
  Omni Award: Bronze, Educational Category; Bronze, Government Category.
  This course is the last in a series of three courses focusing on the Assessment and Authorization of information systems under the National Industrial Security Program (NISP).

- **Need-to-Know Security Training Video**
  Horizon Interactive Award: Bronze.
  A short refresher on the fundamental Need-to-Know security principle.

- **Developing a Multidisciplinary Insider Threat Capability**
  Horizon Interactive Award: Bronze.
  This course equips Insider Threat Program Management personnel with the knowledge, skills, and abilities required to assemble an insider threat team. This training is in compliance with DoD Directive 5205.16, The DoD Insider Threat Program, Enclosure 2 (Responsibilities).

- **Exterior Security Lighting**
  Horizon Interactive Award: Bronze.
  This course provides the student with a basic comprehension of exterior security lighting, to include definition, purpose, planning considerations, and application for the protection of Department of Defense assets.

- **Intelligence Oversight Course**
  Horizon Interactive Award: Bronze.
  This is an interactive, eLearning course that outlines the regulations concerning the collection, retention, and dissemination of intelligence information related to U.S. persons.

DSS employee completes Harvard Program

Frank Malafarina, DSS Counterintelligence directorate, recently completed the Fellowship in National Security at the John F. Kennedy School of Government, Harvard University. The postgraduate research fellowship provides a select group of military officers and civilians from the Department of Defense and members of the U.S. intelligence community a venue in which to study and critically evaluate foreign and defense policy, and a range of national security and homeland security issues.

"There is something to learn from everyone you interact with at the Harvard Kennedy School (HKS) and the National Security Fellows (NSF) program," Malafarina said. "In the NSF program, you interact with students and professors from all over the world on a daily basis.

"It is interesting to see how very smart people can come to very different conclusions based on the same data," he continued. "But it's important to listen to everyone's point of view in order to develop and negotiate workable solutions to complex issues."

As part of his year-long academic fellowship, Malafarina studied and researched a broad array of public and global issues concerning national security policy; domestic, regional, and global environments; interagency, intergovernmental, and multinational planning and execution; and leadership and operations in the public, private, and nonprofit sectors. His academic efforts concentrated on gaining a greater understanding of threats to national security and applicable government policy options to counter these threats.

Malafarina was part of a three-person team that conducted research into autonomous weapons systems, examining the widespread introduction of these systems into military operations and the need for the international community to assess the sufficiency of current international laws and norms to govern their use. The team focused on the applicability of principles, such as sovereign immunity, and the inherent right of self-defense to autonomous weapons systems. The team briefed their research to senior Air Force and Navy leaders in Washington D.C., entered an abbreviated version of their research paper

Frank Malafarina (right), DSS Counterintelligence, stands with DSS Director Dan Payne in front of the statue of Reverand John Harvard on the grounds of Harvard University.

into the Chairman of the Joint Chiefs of Staff National Defense and Military Strategy Essay Competition, and are pursuing publication of the research paper in its entirety.

"The research data necessary to solve complicated problems is available to those willing to put in the time and effort," Malafarina noted. "The tougher the problem the more a leader needs to take the time to think strategically."

After completing the program, Malafarina will be complete a joint duty assignment in the Office of the Under Secretary for Intelligence. He encourages others to participate in the program.

"The Harvard Kennedy School and the National Security Fellows program was the best academic experience of my life," he said, "and I highly recommend it to DSS personnel willing to put in the time and hard work necessary to excel in the program."

Employees receive recognition for contributions to CI and security

Two DSS employees were recognized by DoD for significant contributions to the Defense Intelligence Community's counterintelligence (CI) and human intelligence (HUMINT) missions. The director of the Defense Intelligence Agency presented the awards.

Winners of the DoD CI and HUMINT awards for 2017 were:

- CI Training & Education—Individual: **Rebecca Morgan, Center for Development of Security Excellence**
- CI Training & Education--Team: **DSS CI Cyber Division with the DoD Joint CI Training Activity (JCITA)**

While serving as curriculum manager for both Counterintelligence Awareness and Insider Threat disciplines at CDSE, Morgan "excelled in meeting the training and education needs of the community and stakeholders. Through Morgan's efforts, CDSE became the sole provider of comprehensive CI Awareness, Insider Threat Awareness, and Unauthorized Disclosure training for the DoD, Intelligence Community, other federal agencies, and cleared industry, which contributed to the protection of national security interests. Over one million students accessed Counterintelligence Awareness or Insider Threat Awareness training during calendar year 2017."

The DSS/ JCITA Team implemented programs that instilled technical knowledge throughout DSS, allowing the agency to respond and engage foreign intelligence entity threats in cyberspace, preventing the future loss of critical technology.

National Counterintelligence (CI) and Security Awards

Employees of the Defense Security Service received recognition in four categories of the 2018 National Counterintelligence (CI) and Security Awards at a ceremony hosted by the Director of the National Counterintelligence and Security Center (NCSC). The NCSC recognizes individuals and teams across the Intelligence Community (IC) who made significant contributions to CI and security missions during the previous calendar year.

There are 12 categories for which nominations can be made, and this year, three individuals and one team from DSS won:

- CI Investigations - Individual: **Alberto Rodriguez (Cypress Field Office, Western Region)**
- Education/Training - Individual: **Rebecca Morgan (Center for Development of Security Excellence)**
- Industrial Security - Individual: **Richard Lawson (Philadelphia Field Office, Northern Region)**
- Industrial Security - Team: **Phoenix Field Office CI Team (Western Region)**

Rodriguez was recognized for "his critical thinking skills by identifying nearly 1,000 potential foreign collection attempts targeting DoD classified, export controlled, and critical technologies controlled by the International Traffic and Arms Regulations (ITAR). These reports answered critical intelligence gaps concerning numerous top-tiered countries and

provided the IC with powerful insight into national security threats affecting cleared industry. In addition to detecting and disrupting foreign intelligence activities within his area of responsibility, Rodriguez conducted proactive educational outreach to industry by providing 22 comprehensive CI threat awareness briefings to over 1,000 cleared contractor employees."

While serving as curriculum manager for both Counterintelligence Awareness and Insider Threat disciplines at CDSE, Morgan "excelled in meeting the training and education needs of the community and stakeholders."

Lawson was recognized for leading a "highly educational and impactful collaborative effort to create the Risk Based Analysis Tool (RAT), which significantly improved field office processes in regards to employing a risk-based approach. Successfully integrating CI and security, the RAT has resulted in more efficient prioritization, better collection emphasis, and the mitigation of potential adversarial threats, directly aligning with agency strategic goals and increasing industrial security at a fundamental level. Lawson also demonstrated excellent performance by identifying 59 potential foreign collection attempts targeting DoD classified, export-controlled, and critical technologies protected by the ITAR."

The DSS Phoenix CI Team collected 4,923 cleared industry suspicious reports, published 605 intelligence information reports, and referred 640 reports for awareness or action that produced 80 investigations, source operations, and multiple arrests. "The team identified cutting-edge technology at a small composite materials firm and, on their own initiative, provided tailored CI training that ensured the company maintained its leading edge in this new technology, and guaranteed DoD maintained its technical advantage. They also partnered with over 50 government agencies in efforts that ultimately led to the identification of 80 sources or subjects for federal investigations or intelligence operations, and

Island Security

DSS Director Dan Payne (center) stands with DSS employees from the Western Region, San Diego Field Office, Hawaii Resident Office and members of the Aloha Industrial Security Awareness Council during a recent trip to Hawaii.

Program manager authors book to help organizations improve customer service

One could argue that poor customer service seems to be the norm, rather than the exception in today's business world. Customers may interpret poor customer service as lack of interest by the company or that they don't care about taking care of their customer.

Rather than get mad, Joe Wolemonwu, a program manager in the Industrial Security Integration and Application directorate, decided to do something about poor customer service by writing a book explaining the importance of using knowledge management to improve customer service. His book, Leveraging Knowledge Management for Efficient Customer Service: The Importance of Knowledge Management In Providing Improved Customer Relationship Management, covers the issue of poor customer service, its impact on the growth of an organization and how organizations can leverage knowledge management to provide an efficient customer service experience.

"Knowledge Management is the process of capturing, distributing, and effectively using knowledge," said Wolemonwu. "If organizations know their customers, know what they need and figure out a win-win method that benefits customers while organizations maintain a profit, I believe that customer satisfaction can hit an all-time high."

He wrote the book because "of the bad customer experience I encountered over the years, as have many of my friends and colleagues who have shared similar experiences," he said. "I decided to share my personal experience as well as that of my friends, and offer solutions using knowledge management as a tool."

Wolemonwu noted that people encounter customer service issues every day, and not just in retail situations. "Your boss is a customer and your peers are customers," he said, noting that knowing your customers is fundamental for efficient customer satisfaction. "We have what it takes, we just need to use the data to do better at customer service."

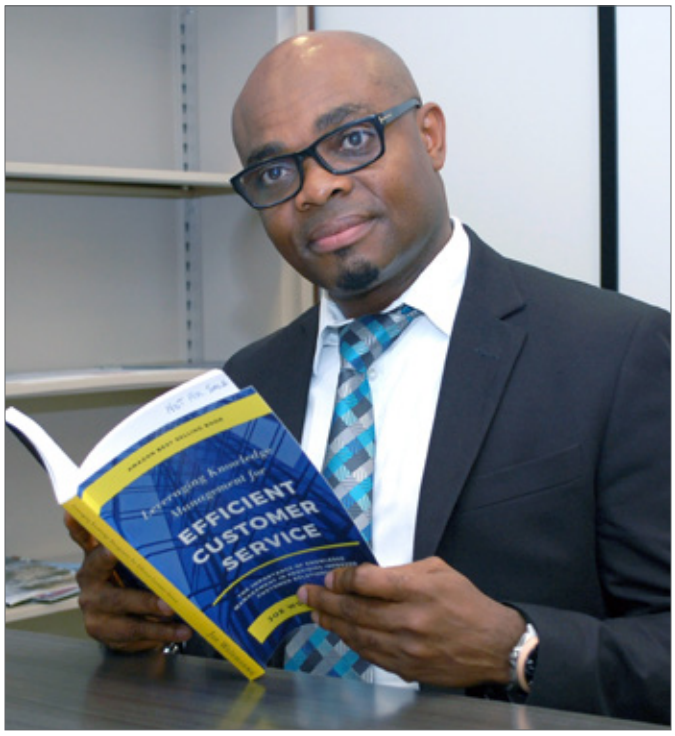
In developing his book, Wolemonwu spoke to numerous people about customer service and discovered that

> "Your boss is a customer and your peers are customers,...knowing your customers is fundamental for efficient customer satisfaction."

it boiled down to a question. "I found that often the solution is in the hands of the person who complains," he said. "Just ask them – what can I do to solve the problem?"

But traditionally, he noted that most people don't pay attention to the complainers; but rather they go on the defensive. "Customers feel ignored and feel that businesses don't care," he said.

"I'm planning to write a sequel of this book because it is an important topic in our society today."



Joe Wolemonwu, Industrial Security Integration and Application, leafs through the book he authored.