Volume 4, Issue 2 Official Magazine of the Defense Security Service

DSS ACCESS

Senior Leader Annual Meeting | Awards Ceremony | DSS Welcomes ...

SUMMER 2015

Volume 4, Issue 2

DSS ACCESS

Published by the Defense Security Service
Public Affairs Office

27130 Telegraph Rd.
Quantico, VA 22134
dsspa@dss.mil
(571) 305-6751/6752

DSS Leadership

Director
Stanley L. Sims

Deputy Director
James J. Kren

Acting Chief of Staff
La Shawn B. Kelley

Chief, Public Affairs
Cindy McGovern

Editor
Elizabeth Alber

Graphics
Steph Struthers

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

From the Director

Happy Spring! As I write this, Spring has finally arrived in the Quantico area and the blossoms and flowers are putting on a stunning display. And best of all, baseball is back.

I mention spring because April was a significant month for DSS. On April 1, 1972, Air Force Brig. Gen. Joseph Cappucci assumed the duties as the first director of the Defense Investigative Service (DIS). Cappucci was the former director of Air Force Office of Special Investigations. Then on April 18, 1972, the DIS charter (tasks, responsibilities, authority) was published in DoD Directive 5105.42. This designated DIS as a separate operating agency under the direction of the Secretary of Defense.

So historically, DSS traces its origins to April 1972. But April is significant for another more somber reason. On April 19, 1995, DIS/DSS lost five colleagues and friends in the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Okla. Five colleagues who were just ordinary people doing their ordinary jobs that fateful day.

This year, I was able to attend the 20th anniversary memorial service held at the National Memorial and Museum. It was my first time to visit and I was humbled and moved by the experience. I was able to meet with family members of each of our employees and I can tell you, they remember the events of 1995 as if it happened just yesterday. Their emotions are still raw and the hole the loss of their loved ones left in their lives clearly visible. Several of the family members continue to reside in Oklahoma, but others came from Florida and Nebraska to remember and honor their brother, father, mother.

As I said, these were ordinary people doing their jobs — just like every DSS employee does every day. They were dedicated, hardworking people who believed in what they were doing, they believed in the mission of the agency, and they were proud to serve their country. The men and women of today's DSS are cut from the same cloth.

Jack Donnelly, DIS Director in 1995, said, "The terrible day brought sadness that will never fade, but it also forged a bond between those of us involved that will never break."

He was right, and our charge is to carry on in their memory, to ensure their sacrifice is not forgotten. And our history, the history of DSS, is forever linked to the Oklahoma City Field Office and the lives of Harley Cottingham, Peter DeMaster, Norma Jean Johnson, Larry Turner, Robert Westberry, and their families.

Thanks for all you do for DSS and to advance the security of our nation.


Defense Security Service
Strategic Plan 2020
Our Agency, Our Mission, Our Responsibility

Strategic Plan **2020**: Strategy to Action

by Dr. Kim Colon
Strategic Management Office

Strategic Plan 2020, released in late February, is a dynamic document that defines the mission of the Defense Security Service and provides a road map of five strategic goals the agency will work to attain in accomplishing the mission over the next five years.

Strategic objectives were developed for each agency goal, with associated performance goals for agency employees to use in measuring success. The following five strategic goals are critical for positioning the agency for continued effectiveness and success in the future.

Goal 1: Strengthen capabilities to continually identify, evaluate, and mitigate risk to the DoD and the national industrial base.

DSS will focus on ways to best position itself to mitigate risks faced by cleared industry and DoD security professionals to ensure the protection of the Nation's critical technology, information and warfighting capabilities.

Goal 2: Enable government and industry stakeholders to proactively manage risk.

As a security oversight and educational agency, DSS mitigates risk by helping those stakeholders strengthen their defense through quality education and training, and providing best practices that help our partners improve their own risk management processes.

Goal 3: Strengthen national security partnerships.

With the increasing need for information sharing and working jointly with multiple security organizations, DSS is focused on expanding and strengthening the key relationships it has already established within the intelligence and security communities.

Goal 4: Empower a mission-driven workforce responsive to the changing environment.

For DSS to succeed, it needs a workforce that is flexible, reliable, innovative and dependable. To that end, DSS is committed to providing opportunities to excel through training, mentorship and increased responsibility.

Goal 5: Provide enterprise solutions to improve operations and performance management.

For several years, the federal workforce has been operating in an environment of doing more with less, requiring strategic planning for efficient use of resources. DSS is committed to providing employees with the proper tools to complete their jobs, which supports the growth of efficiency and compliance with standards.

While continuing to work toward the accomplishment of agency mission goals, it's important to recognize we want to achieve greater:

Integration • Transparency • Collaboration • Alignment

Incorporating these factors into individual and agency achievements inherently brings us closer to mission accomplishment. An example of incorporating all four factors into an activity could be the participation in a cross-functional working group (i.e. National Industrial Security System).

All DSS personnel see themselves in the Strategic Plan

This is a "top-down" and "bottom-up" document. Developed as a road map in guiding us toward mission accomplishment, the strategic plan can also be used during the establishment of individual performance plans, midpoint reviews and performance evaluations. Aligning the agency goals and objectives to performance plans will alleviate much uncertainty as to whether an employee is working toward agency mission accomplishment.

In preparing to move into the implementation of the Strategic Plan, I share the following thoughts:

- We spend much of our time and energy focused at tactical and operational levels. The Strategic Plan will hopefully allow all employees to take a step back and see what is on the horizon.

- Executing strategy is more than a pass/fail notion — it is not about going from "red" to "green." Execution is also about defining what may be preventing DSS from moving forward and why. Taking stock of where you are and recognizing the need for additional resources, systems, support or guidance to keep us moving forward is essential. Sometimes this may require abandoning an initiative in which a significant effort has been made.

- Moving beyond silos (i.e., Counterintelligence, Industrial Security Field Operations, etc.) is also a real issue. Sometimes it takes moving across functional areas to make real progress. It is incumbent upon all DSS employees to identify areas where mission success could be hampered by duplication of efforts, failure to align, or failure to coordinate.

- We have done a tremendous job creating this plan, which also gives industry and agencies a better understanding of where DSS is headed. However, this is just a starting point and there is more work to be done. Let's keep the momentum going as we head into the implementation phase of Strategic Plan 2020.

As time passes, the plan will be reviewed and adjusted as needed to incorporate new security policies, evolve for the changing security environment, or to address other strategic planning developments necessitating new direction and targets.

Leadership team focuses on changes, DSS business and executing strategy

The DSS Senior Leadership team spent three days in late March at Airlie House in Warrenton, Va., for their annual meeting. Each of the three days had a theme with a series of presentations or discussions building upon it. In his opening remarks on Day One, Stan Sims, DSS Director, noted the addition of senior leaders in the following key positions: Director of Industrial Security Field Operations, Gus Greene; Director of Industrial Policy and Programs, Fred Gortler; and Chief Information Officer, Craig Kaucher.

"Each brings a unique skill set, a fresh look and renewed enthusiasm," said Sims in his introduction. "We scheduled this annual meeting to ensure we had these positions filled and to get them off on the right foot."

The theme for Day One was "Changing Security and Risk Landscape." Perhaps the biggest change for DSS in that regard is the new mission assigned to DSS in December 2014 to establish the Department of Defense Insider Threat Management and Analysis Center (DITMAC). Matt Guy of the DITMAC focused his update on planning milestones, which include a physical relocation from Quantico, hiring additional staff and procuring necessary equipment.

Also critical to the DITMAC's success is defining the process flow of information, capturing roles, responsibilities, major inputs and outputs and relationships across the Department. Sims emphasized that the DITMAC provided an enterprise level management capability that did not involve DSS doing the jobs of the various components.

"There are many, many pieces to this new mission," said Sims. "We are still getting our arms around it, but I know in the end, we'll get this done."

Jen Gabeler of the Counterintelligence directorate gave a presentation on integrating counterintelligence into the facility clearance process. Gabeler said a threat integration working group with representatives from across DSS wanted to establish thresholds for counterintelligence review of facility clearance determinations. Ultimately, the goal is to use the intelligence information available within Counterintelligence to tailor security vulnerability assessments of cleared facilities.

"We want to know which people to talk to, about which program at which facility," Gabeler said. "We could then use that information to develop a dynamic facility of interest list that changes based on the risks and the threat. We can also assess the threats to critical technology resident at a facility prior to the facility entering the National Industrial Security Program and establish a relationship early on."

The theme of Day Two was "The Business of DSS." In setting the stage for the day, Sims said DSS is a small agency operating in a resource-constrained environment. As a result, it was important to prioritize agency activity but also to do so with an eye on the future.

The first presentation focused on the challenges of developing leaders across the agency, 'how many leaders we need, what kind, where, with what skills, traits and behaviors.' The need to identify and develop leaders is particularly critical at DSS, said Larry Cunningham, due to the high number of personnel eligible to retire in the next five years; many of whom are subject matter experts in their fields.

Cunningham returned to DSS from retirement to assist in the establishment of a Leadership Advisory Board (LAB) (see related article on page 18). The LAB is comprised of members from across DSS with the goal of developing a pipeline of personnel capable of carrying out the agency's goals, missions and objectives. "We want to cultivate a leadership culture throughout DSS that addresses the leadership competencies expected," he said. "We also want to provide education, training and development opportunities to these leaders because they are our leaders of the future."

Cunningham also discussed specific deliverables for the LAB such as a leadership strategy roadmap, timelines, measures, and strategy. While the LAB focused on future leaders, the Gang of Four focused on current gaps across the agency and in filling them. The Gang of Four, the

deputies of Field Operations, Counterintelligence, Policy and Programs and the Center for Development of Security Excellence, recently expanded its membership to include Financial Management.

The Gang of Four conducted a series of visits to field offices across the country to identify gaps between the field and headquarters and also between individual regions and field offices. From these visits, the Gang of Four prioritized the gaps and developed a series of recommendations to fill them. For instance, one gap was the lack of an agreed upon definition of risk management; another is the appropriate level of standardization versus field autonomy.

While acknowledging the need for consistency across DSS, the Gang of Four noted that each region is unique and wanted to allow for local decision making and creative solutions. The solution, said Jim Kren, Deputy Director, might be sharing a clear, concise definition of risk management.

Another suggested solution was to tie recommendations back to the DSS Strategic Plan and its series of goals and objectives. The Gang of Four will continue to meet and visit the field and develop a comprehensive communication strategy to share their findings.

Another new mission for DSS is National Interest Determinations (NIDs) for companies operating under Foreign Ownership, Control or Influence. The requirement for a NID is not new, but DSS now has the ability to propose a NID on behalf of the Government Contracting Activity (GCA) if the FOCI company will require access to proscribed information while operating under a Special Security Agreement.

Lynda Mallow, acting director of Industrial Policy and Programs, said there are roughly 27 companies in the NISP that would require a NID, but the contracts and companies in question are often high-visibility, and the process in the past has been cumbersome and slow. One of the reasons, she said, was the lack of information or understanding on the part of the GCA. The DSS goal then is to develop a process to streamline the steps but also provide analysis and data to the GCA to allow them to make an informed NID.

Day Two ended with an in-depth look at the DSS budget for FY15, as well as the projections for fiscal years 2017 to 2020.

The theme for Day Three was "Strategy to Action." The Strategic Management Office (SMO) published the DSS Strategic Plan 2020 in March (see related article on page 5) and the discussion focused on implementation of the plan. Dr. Kim Colon of SMO gave an overview of the performance goals associated with the plan, along with an overview of the implementation plan from strategy oversight down to individual actions and measurements. She noted a total of 115 performance goals for completion over the course of the plan and discussed the breakdown by office.

Sims noted that every DSS employee should have a copy of the plan and know how their jobs support the agency's five strategic goals. "This is a very readable document," he said. "It's short, concise and every employee should understand where they fit into the agency and its goals."

Also included in the third day's presentations were Alternative Dispute Resolution (ADR) and Succession Planning. Dr. Carey Williams of the Equal Employment Office said ADR is an important tool to resolve workplace disputes that can negatively impact the agency's mission and goals. During his presentation, Williams said ADR is often misunderstood but can in fact foster clear communication and find areas of mutual interest and understanding between the parties.

Sims addressed the issue of succession planning and how important it was for managers and leaders to engage their employees on their career progression and development. He said the goal was to have a pipeline of employees ready to assume leadership responsibility as the opportunities presented themselves. "You know my motto, people first, mission always," he said. "Both ADR and succession planning are about people taking care of people. ADR can resolve issues at the lowest levels. Succession planning ensures we are recognizing those high achievers who are ready to move into leadership positions."

In his closing remarks, Sims said while each of the three days had a theme, the overall message he wanted attendees to take away was people. "People first should always be our enduring theme," he said. "We didn't talk process this week; we talked about our collective mission and how to achieve it. At the end of the day, it's not what we do, but why we do it; why does DSS matter?"

Sims charged the senior leadership team with not resting on their laurels and continuing to advance the agency's mission. "We will be measured by the actions we take," he said. "Remember, it's our agency, our mission and our responsibility."

PHOTOS FROM TOP: Karl Hellman, Western Region director, talks about best practices. Guest speaker Dr. Gerald Suarez (left) works with Mark Allen, DSS Counterintelligence, during a seminar on "Moving From Strategic Thought to Strategic Action." Rebecca Allen, former DSS Chief of Staff, listens to a briefing.

Annual award ceremony recognizes the 'best of the best'

The fourth annual Director Awards ceremony was held in late March and coincided with the Industrial Security Field Operations Supervisor's Training. The standing-room-only crowd recognized the 2014 Excellence in Innovation Award as well as the Team and Employee of the Year for 2014.

In his opening remarks, Stan Sims, DSS Director, said the Director Awards program was one of the things he is most proud of since joining the agency. "There is nothing more rewarding as a leader than to recognize your employees. Employee recognition is a motivating factor — it helps people develop and strive to do better," he said. "All of the people we will recognize today are working to make DSS a better organization and by extension, contribute to national security."

He encouraged all managers and leaders in the audience to incorporate employee recognition into their daily routines — whether a simple thank you, or pat on the back.

Sims added that it was not possible to formally recognize everyone at DSS doing good work, but ceremonies such as this allow him to recognize those employees who go above and beyond their normal duties in front of their peers and colleagues. He said the agency would continue to look at ways to improve the award program and other ways to recognize deserving employees.

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

EMPLOYEE OF THE YEAR

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

The winner of Employee of the Year for 2014 was Andrianna Backhus, Industrial Security Field Operations.

Backhus was nominated for her "unrivaled excellence, dedication, and outstanding accomplishment in support of DSS and the National Industrial Security Program." Backhus was instrumental in developing, managing, and sustaining strategic partnerships within DSS, and with industry and other government agencies to integrate improvements to service delivery, policy, and processes.

Backhus' impact is government-wide through her extensive involvement in key roles, to include the development of the National Industrial Security System (NISS), initially as an action officer and currently as the program manager for the non-material solution implementation.

Employee of the Year Andrianna Backhus (left), Industrial Security Field Operations, stands with DSS Director Stan Sims.

Backhus is also the quality assurance action officer managing the DSS Rating Matrix and its implementation in industry. Both of these efforts demonstrate her ability to develop customer-focused, trend setting improvements while building partnerships and improving collaboration between people and organizations.

In presenting the award, Sims said he first met Backhus over three years ago when she was an Industrial Security Representative in the Capital Region. "I knew then we had a rock star," he said. "She knew what she wanted to do and has been leading in the agency ever since." Sims added that the non-material solution to the NISS is about changing processes. One of Backhus' tasks with NISS moving forward will be to train the workforce on using the system and adopting the new processes. "NISS is the future of DSS," Sims said.

In her remarks, Backhus said she was proud and humbled by the award. She said she didn't know what she was getting into when she volunteered to be part of the NISS team, but her field office chief challenged her to get involved. "While I've been here at DSS, I've been fortunate to have mentors and leaders who challenge me and provide me with unique opportunities. But she said, "It's the DSS employees across the agency who inspire me to be a better person and help me learn. I am constantly impressed by the intelligence, confidence and dedication DSS employees' exhibit every day."

The following individuals were also nominated for Employee of the Year:

Pete DeCesare, Center for Development of Security Excellence.

As curriculum manager, DeCesare developed and built partnerships with DSS Counterintelligence directorate, Office of the Under Secretary of Defense for Intelligence, National Insider Threat Task Force (NITTF), and National Counterintelligence Executive (NCIX). All played an integral role in his development of a series of CI courses.

DeCesare promoted the CDSE insider threat training and, as a result, NITTF and NCIX adopted this training as the premier source for the Intelligence Community and federal agency personnel. This partnership may reach up to two million users. Additionally, the partnership led to increased information sharing between DSS and NCIX, further increasing CDSE's reach across the Intelligence Community.

John Massey, Operations Analysis Group (OAG).

Massey excelled in customer focus and process improvement. He had a significant impact in executing each of the agency's core values but his most noteworthy accomplishments resulted from his dependability. He leveraged his support from, and responsibilities to, each DSS directorate to build and execute trend setting initiatives that strengthened DSS's mission effectiveness and efficiency.

His customer focus, process improvement and dependability served as the OAG catalyst. As a result, the Director for Defense Intelligence (Intelligence & Security) requested a monthly OAG update that serves as a model for DSS and has garnered support at the highest levels in the Office of the Under Secretary of Defense for Intelligence.

Allyson Renzella, Industrial Policy and Programs.

Renzella excelled at providing customer focus, building relationships and collaborating with DSS colleagues and external stakeholders. Her efforts, partnerships, skills and proactive efforts are invaluable to the Foreign Ownership, Control or Influence (FOCI) Operations division. She was instrumental in identifying critical security vulnerabilities during a routine assessment of a highly visible FOCI company. Renzella volunteered her services to join the vulnerability assessment providing Industrial Security Field Operations with much needed subject matter expertise and support.

Christina Vargo, Counterintelligence Directorate.

Vargo has a passion for cyber analysis and intelligence which are demonstrated through her initiative and drive. She applied critical thinking techniques to a wide variety of items and uses reasoning skills to determine solutions.

She was a key player in outreach sessions with cleared industry. This direct support led to a new feedback mechanism to improve product lines and has had a direct impact on reporting from cleared companies. It also led to the successful identification of numerous penetrators and gives the public/private enterprise a holistic view of the cyber threat.

Kristin York, Business Enterprise.

York's technical expertise, professionalism, collaboration, and customer interaction led to the successful completion of the DSS headquarters project on time and under budget. She assembled and managed a cohesive, highly functional, multi-disciplined project team.

Through her continuous collaboration with the team, she overcame design issues, weather delays and other issues that would have impacted schedule and cost to the agency. York's customer focus and her management of the project provided DSS with a state-of-the-art facility for years to come.

Members of the 2014 Team of the Year, Command Cyber Readiness Inspection (CCRI) team from Industrial Security Field Operations, stand with DSS Director Stan Sims (center).

TEAM OF THE YEAR

The Team of the Year award recognizes teams who, as a group, exhibit the highest standards of excellence, dedication, and accomplishment in support of the DSS mission.

The 2014 Team of the Year is the Command Cyber Readiness Inspection (CCRI) team, Industrial Security Field Operations.

The team made unprecedented advances and process improvements to bolster cyber readiness at cleared contractor

facilities involved with DoD classified networks, gaining significant credibility from internal and external stakeholders.

In March 2014, U.S. Cyber Command approved the first of five DSS teams to begin conducting CCRIs. By demonstrating their credibility and expertise, DSS CCRI teams will conduct roughly half of the CCRIs at National Industrial Security Program contractor facilities in FY15 with no oversight from the Defense Information Systems Agency.

Overall, the DSS CCRI team's efforts have significantly enhanced national security by positioning and enabling these contractor facilities to proactively identify and mitigate vulnerabilities, and prevent future occurrences to affect the most sensitive classified information systems. Since DSS began conducting CCRIs, there has been improved cooperation between industry and government agencies, and increased program effectiveness and efficiencies.

In presenting the award to David Scott, team representative, Sims said the CCRI mission was near and dear to him. "We took this new mission with no additional resources because it was the right thing to do," he said. "We took the mission because we knew we had the expertise and the experience working with industry to do this right."

Sims noted that the DSS CRRI teams are now the most experienced teams conducting CCRIs. "Since we took this mission, we had one [SIPR] node fail their CCRI. Just one. Before we got involved, about 40 percent of industry nodes failed," he said. "It's because we are out in industry all the time, we know what's going on at these facilities and we work with them to resolve the issues before they fail. That serves national security."

In accepting the award on behalf of the team, Scott gave credit to the information systems security professionals across DSS who

Command Cyber Readiness Inspection Team Members:

May Braganza, Information Systems Security Professional Team Lead, *San Diego*

Elisabeth Bruinsma, Senior Industrial Security Specialist, *San Antonio*

Robert Burrows, Information Systems Security Professional, *Virginia Beach*

Anthony Carbone, Cyber Team Lead, *Virginia Beach*

Darnell Carlisle, Senior Quality Assurance Action Officer, *Field Operations*

Victor Castillo, Information Systems Security Professional Action Officer, *Field Operations*

James Cole, Information Systems Security Professional, *Alexandria*

Curtis Cook, Information Systems Security Professional, *Hurlburt Field*

Diane Craig, Senior Industrial Security Specialist, *Mt. Laurel*

Joseph Delarosa, Information Systems Security Professional Team Lead, *Chantilly*

Steve Eisenberger, Industrial Security Specialist, *Philadelphia*

Robert Ems, Information Systems Security Professional, *Huntsville*

John Forster, Information Systems Security Professional, *Pittsburgh*

James Gillespie, Industrial Security Specialist, *Philadelphia*

Michael Irvine, Industrial Security Specialist, *Alexandria*

Monique Jacob, Information Systems Security Professional, *Hanover*

Wayne Lajoie, Industrial Security Specialist, *Chantilly*

John Long, Industrial Security Specialist, *Syracuse*

Renee Lumpkin, Information Systems Security Professional, *Atlanta*

William Mendez, Information Systems Security Professional, *Westbury*

Susan Miller, Information Systems Security Professional, *Virginia Beach*

Derek Mueller, Information Systems Security Professional, *Camp Hill*

Chad Puffer, Information Systems Security Professional, *Syracuse*

David Rees, Information Systems Security Professional, *Phoenix*

Kevin Roberson, Information Systems Security Professional, *Morrisville*

Kelly Schlienger, Information Systems Security Professional, *Chantilly*

David Scott, Senior Information Systems Security Professional, *Office of the Designated Approving Authority*

James Sexton, Information Systems Security Professional Team Lead, *San Diego*

Dustin Sievers, Information Systems Security Professional, *Virginia Beach*

Gary Sims, Information Systems Security Professional, *St. Louis*

Tyquisha Summerville, Office of the Designated Approving Authority

Scott Taylor, Information Systems Security Professional, *Hanover*

Ehren Thompson, Industrial Security Specialist, *San Diego*

Kerry Waldrip, Industrial Security Specialist, *Irving*

Cheryl Webster, Information Systems Security Professional, *Huntsville*

embraced the challenge. "Each one had to complete rigorous training, obtain certification, participate in inspections that DISA monitored and evaluated and this was all on top of their normal duties. Each team member has done everything we asked of them."

Scott also said the team worked with Government Contracting Activities to reduce the risk at the contractor facilities, which ultimately led to fewer vulnerabilities. He said the biggest challenge now was managing the waiting list of employees eager to participate in the CCRIs.

The following were also nominated for Team of the Year:

2014 Virtual Conference Team, Center for Development of Security Excellence.

Due to budgetary concerns that caused a hiatus of the DoD Worldwide Security Conference, the team produced the first DoD Worldwide Security Virtual Conference. The virtual format allowed over 1,000 security personnel to attend remotely and still have direct contact with security community leaders and policy experts. It also saved as much as one million dollars in travel, lodging and prep costs. The team included stakeholders from across the community and connected the needs of attendees with policy makers and leadership.

Administrative Support Contract Team, Business Enterprise and Office of Acquisition.

This team was nominated for the re-compete of the agency's administrative support contract. This committed, cohesive team rewrote the performance work statement, standardized tasks and updated qualifications. While sequestered, the team considered each proposal and evaluated them according to the solicitation criteria and the contracting officer's instructions.

The result was a successful contract award that saves DSS six million dollars over the next five years. The team's commitment to fairness and their steadfast desire to serve the best interests of DSS resulted in a successful award, with no protest, and a transition with the fewest negative impacts.

Cyber Operations Team, Counterintelligence.

This team developed and implemented innovative processes that found new cyber tradecraft that foreign actors use to compromise contractor networks. The team produced cyber leads that led to investigations and operations by the law enforcement and the counterintelligence communities.

The team's cyber alerts led to the identification of several previously unknown penetrations of contractor networks. The team supported the secure operations of our nation's critical assets, helping maintain our technological edge and defense advantage.

Defense Civilian Intelligence Personnel System (DCIPS) Team, Human Capital Management Office.

The team, comprised of two employees, oversees the DCIPS performance management cycle. It is committed to delivering the highest level of customer service and building partnerships across the agency. The team ensures that every DSS employee understands the DCIPS performance cycle, the SMART objective methodology and alignment of objectives to achieving mission success. They consistently deliver quality products and services that require a level of dedication, dependability, collaboration and accountability.

National Industrial Security System (NISS) Team Members:

Industrial Security Field Operations

Andrianna Backhus
Sarah Beauregard
Mike Brown
James Cole
Ryan Deloney
Ryan Dennis
Dustin Dwyer
Lauren Firich
John Forster
Kelly Grace
Jeremy Hargis
Clarence Hollingsworth
Nicholas LeVasseur
Jennifer Norden
Shobha Ramaswamy
Eleanor Rempfer
Andrea Rhodes
Gretchen Runkle
David Scott
Gary Sims
Katy Vachon
Dan Van Aulen
Grant Ward
Leslie Whitaker

Industrial Policy and Programs

Wayne Chin
David Hibbert
Helencia Hines
Steven Lindquist
Lovely Rodriquez
Anne Snellings
Bron Stacey
Ursula Stearns

Counterintelligence

Jeffrey Boick
Ryan Rivera
Charles Zakaib

Office of Acquisition

Summer Wilson

Office of the Chief Information Officer

Diane Brooks-Woodruff
Eric Von Dibert

Program Integration

Andy Branigan
Naimah Ewing

Members of the 2014 Excellence in Innovation of the Year winners, the National Industrial Security System team from Industrial Security Field Operations, stand with DSS Director Stan Sims (center).

Industrial Program Tiger Team, Industrial Policy and Programs (IP).

This team bridged the gaps and built stronger bonds between the field offices and headquarters. A survey of the field found knowledge gaps about the mission of the directorate. To bridge these gaps, IP established a "Tiger Team" of subject matter experts. The team visited the field to familiarize them with the IP mission, functions and scope. The efforts supported and advanced the agency's mission.

EXCELLENCE IN INNOVATION OF THE YEAR

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

The 2014 Excellence in Innovation of the Year Award was presented to the National Industrial Security System (NISS) Team, Industrial Security Field Operations.

This team led a transformational modernization of DSS processes and technology that support National Industrial Security Program oversight and our national security mission. The team mapped new processes, reduced process steps and streamlined agency initiatives. This effort included the collaboration of over 100 subject matter experts from across DSS, industry, and other government agencies. The result is an innovative way of conducting business that will benefit DSS, industry, and government stakeholders for years to come.

In presenting the award, Sims called the NISS one of the most important projects DSS is working on. "If we do this right, and we will, we will influence the entire National Industrial Security Program," he said. "It will use 21st century technology to automate manual processes and integrate existing databases that right now, cannot communicate."

In accepting the award on behalf of the team, Ryan Deloney said over 100 DSS employees had contributed to the NISS by sharing ideas, participating in working groups and mapping processes. "NISS is a great example of what 'one DSS' can do," he said. "This really shows how collaboration and communication can advance the agency's mission."

Deloney said he was excited about the process improvements and said he would like to take that energy and apply it to other process improvements across DSS.

In addition to the DSS employees who received a plaque at the ceremony, additional contributors received a certificate signed by Mr. Sims.

The following were also nominated for Excellence in Innovation:

Conversion Team of DoD Security Specialist Course into Collaborative Learning Environment, Center for Development of Security Excellence.

This team transitioned the DoD Security Specialist course from an instructor-led format into a collaborative learning environment. This collaborative team of subject matter experts demonstrated originality, innovation, impact and value. As a result, students have a modern, up-to-date format, and save DoD travel costs and time away from the office.

Virtual Desktop Infrastructure, Office of the Chief Information Officer.

This team developed the virtual desktop expansion program. This technology allows users to have the same desktop at work and at home, which includes files and mapping. The team demonstrated exceptional critical thinking, impact and value in integrating two technologies that enhanced employees' experience at work and in telework environments.

DSS employees remembered in solemn ceremony

April 19, 2015 marked the 20th anniversary of the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Okla. In 1995, the Murrah building housed 23 federal and 10 state agencies.

This year's solemn memorial ceremony drew a huge crowd and number of dignitaries representing those affected agencies, as well as former mayors, governors and even a former president. It also included family members of the five employees of the Defense Investigative Service killed in the explosion: Harley Cottingham, Peter DeMaster, Norma 'Jean' Johnson, Larry Turner and Robert Westberry.

The ceremony opened with a procession of family members and agency representatives led by two pipers from the Drug Enforcement Agency who led them past a row of wreaths representing each agency who lost employees in the bombing.

After pausing for a moment of silence at the wreaths, the procession continued through the field of chairs — one chair for each of the 168 victims — to one of three dais facing the reflecting pool and crowd assembled on the other side.

On the second dais were elected officials to include Sen. James Lankford (R-Okla.), former Mayor Ron Norick and former Governor Frank Keating. Norick and Keating were both in office in 1995 and in fact, Keating had just marked his 100th day in office when the bombing occurred.

Norick recounted taking a phone call from the White House shortly after the bombing and said, at any other time he would have thought someone was playing a joke on him.

But instead he found himself talking to then President Bill Clinton who asked

Sandy Battraell and Sheryl Oriatt, sisters of Harley Cottingham, read the names of the DSS employees killed in the Oklahoma City bombing during the remembrance ceremony. Watching on are (from left) former President Bill Clinton, Oklahoma Governor Mary Fallin, DSS Director Stan Sims and Glenn Westberry, son of Robert Westberry.

him, 'What can I do for you?' "I will always remember his kindness to this city," said Norick.

Keating likewise talked about the sacrifice of those who perished but also the overwhelming response from local, state and federal first responders, as well as the local community, saying, "So many of you gave so much. People went out of their way to share everything they had to make it comfortable for the rescue workers, the firefighters, anyone who was there to help," said Keating.

This outpouring of commitment and generosity became known as the Oklahoma Standard and now serves as a model for other first responders and communities to emulate."

On the third dais were the main speakers for the day each of whom focused their remarks on a different but related theme.

Mick Cornett, current Mayor of Oklahoma City, talked about how the city had changed and said that while the events of April 19, 1995 were the city's darkest hour, its finest hour has lasted 20 years as the city has progressed in ways no one could have foreseen.

Mary Fallin, current Governor of Oklahoma, talked about the Oklahoma Standard and said evil happened 20 years ago, but evil could also be used for good as it had in Oklahoma. She said the progress made to date was due to grace, love and compassion.

Fallin said the events of April 19, 1995 thrust the city and state into a worldwide limelight and the remarkable response from across the state and country gave the community hope and encouragement. "Let us not forget," she said, "Let us commit to reminding future generations of Oklahomans of what happened here."

James Comey, Director of the Federal Bureau of Investigation, talked about the resilience, resolve and hope of Oklahoma City, but also delivered a stark reminder of the commitment of the FBI and federal law enforcement.

Comey noted that those killed in 1995 were ordinary people going about their ordinary day who were transformed by moments that forever altered their lives. "It's not that moment that defines us," he said, "It's what comes next." And what came next for many was to run toward darkness, pain and destruction. "You were strong and unbending," he said.

Comey said life is a search for understanding why bad things happen. He said while one cannot help asking why, one must also ask how. "How can we move forward?" he asked. "Because out of the darkness will come a ray of light."

He added that the Oklahoma Standard was now the American standard and similar acts of kindness and resiliency were evident in New York on Sept. 11, 2001 and in Boston on April 15, 2013. He closed by saying, "The FBI will do all we can to find and stop evil. We will do all we can to keep you safe, that is our standard."

Jeh Johnson, Secretary of Homeland Security, addressed domestic security in his remarks by emphasizing how the Oklahoma City bombing changed national policies. "Today is a day to mourn and

DSS Director Stan Sims (left) extends condolences to Dianne Turner, wife of Larry Turner.

remember those who died here 20 years ago, but this is also a day to say to those who plan to terrorize us, 'no, you cannot.'" Oklahoma embodied that message, Johnson said.

While each of the speakers touched on remembrances and progress, it was Clinton, making his sixth visit to Oklahoma City to attend a memorial service, who delivered the keynote address and assured the audience, the nation remembers. Clinton seemed to speak directly to each family member on their loss, courage, sacrifice and embrace of the Oklahoma City Standard.

"When you strip away all the little things that divide us, it is important to remember how tied we are and how much all Americans owe to Oklahoma City," Clinton said. "You chose farsighted love over blind hatred.

"For 20 years, you have honored the memories of your loved ones, you have inspired us with the power of your renewal, you have reminded us that we should all live the Oklahoma Standard — service, honor, kindness," he said.

"There are still people who somehow think they matter more and they can make a statement by killing innocent people; snuffing out possibility. Who can somehow bend the arc of history," he continued. "They're wrong as long as people like you make the right decisions with your mind and your heart."

Clinton touched on the progress made in rebuilding and revitalizing Oklahoma City, but he also noted, "The material gains were incidental and every family here who lost someone would give it up in a heartbeat to have their loved ones back.

"Not because you forgot the loss of your loved ones, but because you remembered. Not because the pain and loss and love have worn away with time, but because they endure," Clinton said, "and the only way you can redeem your loved ones is to live by the Oklahoma standard."

Following the speeches, Stan Sims, DSS Director, accompanied Glen Westberry, son of Robert Westberry, and Sandy Battraell and Sheryl Oriatt, sisters of Harley Cottingham, to the podium to recite the names of their loved ones and DSS employees killed in the explosion. They joined the procession of readers which included parents, children, grandchildren, sisters and brothers of the 168 victims.

A Q&A with Heather Green,

Director of the Capital Region

Editor's Note: *The following is the third in a series of features on the four DSS regions. In each, the regional director discusses what makes their region unique, the challenges they face and how they address them.*

Heather C. Green assumed her duties as Capital Region Director in January 2013. As the regional director, Green is responsible for the industrial security oversight of approximately 5,000 National Industrial Security Program (NISP) facilities in Maryland, Virginia and Washington, D.C.

She began her career with DSS in 1997 as a Special Agent conducting background investigations prior to moving into the industrial security field.

From 2002 to 2011, she was the chief of the Maryland field office where her responsibilities included management oversight of all aspects of the office, which included leading a team of Industrial Security Specialists and providing security oversight to over 600 cleared contractor facilities.

Prior to assuming her current position, she was the Quality Assurance Manager for Industrial Security Field Operations (IO) where her responsibilities included the oversight of quality, consistency and standardization within IO.

Tell us about the Capital Region. What makes it different from the three other regions?

We are the smallest region in size covering just Northern Virginia, Maryland and Washington, D.C. But with just over 5,000 cleared facilities, we have the most of any of the DSS regions. Of those 5,000, we have the highest number of access elsewhere facilities, the most foreign ownership, control or influence (FOCI) signatories, high profile facilities and industry corporate headquarters of the four regions.

So it is a very complex and large workload, which includes a high number of accredited information systems in a small concentrated geographic area. Because we are close to the headquarters, we often train headquarters personnel on field skillsets and provide many ride-along opportunities.

What are the challenges in the Capital Region?

We have a very junior workforce due to a high level of turnover in the region. This is due to proximity to a lot of other government agencies and our headquarters location, both of which offer multiple government job opportunities. Because we are so close to the headquarters, our staff has many developmental opportunities available to them such as temporary duties, participation on working groups, and exposure to high level meetings, etc.

And because of the complexity of our facilities, our field personnel gain experience in more complex situations rather early in their career. This is certainly a plus for career growth in the region. But it does create one of our biggest challenges: Retaining employees and maintaining the knowledge base within the region. While these are challenges, I think they are also positives as many of our employees stay with DSS and are promoted within the region and headquarters. These employees become force multipliers within the agency as they understand the challenges within the field and apply their field knowledge in their new positions.

The volume of facilities is certainly a challenge with approximately 40 percent of all the cleared facilities in the National Industrial Security Program (NISP) located in the Capital Region. We have to prioritize our workload and actions based on risk as it is important for us to operate ahead of the threat and not behind the vulnerability.

The majority of our facilities are "access elsewhere" facilities, which means they do not possess classified information and perform services at the government customer or prime contractor location. One trend we find with many access elsewhere facilities is that the Facility Security Officers (FSO) are not full-time and often spend a small percentage of their time on security-related responsibilities. Therefore, the Capital Region staff is often

providing advice and assistance, and outreach to those FSOs who are not routinely engaged with the NISP.

We are very well integrated across disciplines in the region which makes this assistance and outreach possible and effective. For instance, our Counterintelligence Special Agents and Information System Security Professionals play a critical part in the oversight role, as well as educating the FSOs and Information System Security Managers.

The Capital Region is very engaged in outreach to industry and we encourage security community participation in the multiple ISAC and NCMS community events throughout the year. And our field offices host open houses and training events for our FSOs.

Is it difficult working so close to the DSS headquarters?

I wouldn't say it is difficult but at times we are called on to assist with short notice initiatives due to our proximity. That can be a challenge. On the other hand, we also have more opportunities to participate in headquarters activities and more high profile agency initiatives. So it gives the region an awareness of larger issues that the other regions may not be exposed to.

We have been working hard to identify and promote professional growth opportunities for our personnel. Our close proximity and relationships with headquarters staff have enabled us to integrate our personnel throughout Field Operations headquarters, as well as in the other directorates within DSS to further expand staff diversification and professionalization. So again, that's a positive for our personnel.

What changes have you made in the region since arriving?

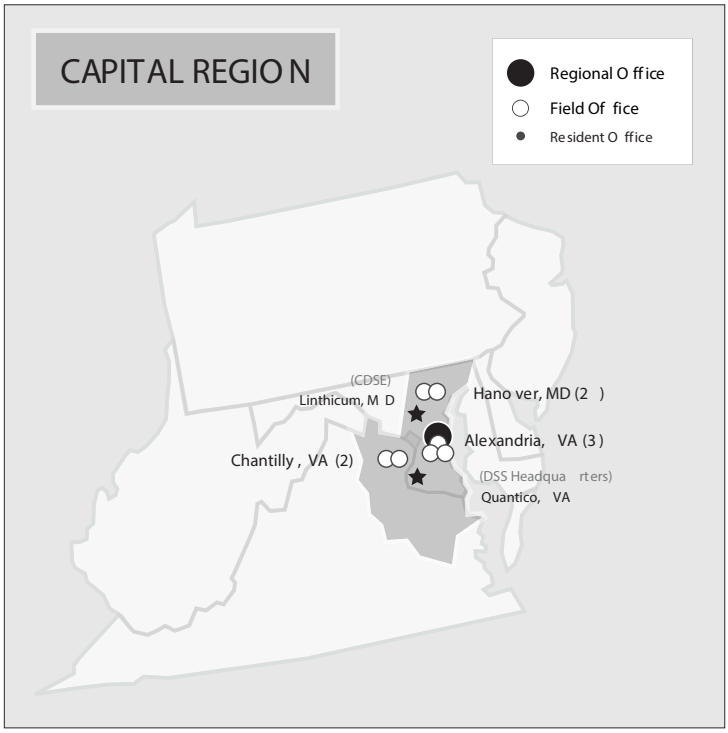
The region has gone through a significant number of changes since I arrived. The most significant changes were the workload balancing, region restructuring and addition of a seventh field office.

The purpose of creating an additional office was twofold. First, we needed to reduce the span of control and workload of the other field office chiefs in the region. With over 5,000 cleared contractor facilities in our area of operations, some of our field office chiefs were managing upwards of 1,000 to 1,100 facilities. This affected our ability to provide support, oversight, and appropriate customer service.

Secondly, over time as different areas of the region have grown, workloads became unbalanced, with some offices carrying significantly heavier or more complex workloads than others. Establishing the new field office allowed us to re-balance workloads across the region. After the transition, all of the field offices within the Capital Region now have an average of 700 to 720 facilities each, with the more complex work also balanced across the seven field offices.

Another significant change was to implement a regional recognition program that enables employees and supervisors to recognize one another for their achievements and contributions towards achieving the region's mission and objectives. The recognition program consists of the Capital Region Star Recognition and the Peer Kudos Recognition.

The Star Recognition is presented quarterly and allows supervisors to nominate those employees who have demonstrated success in any of the region's objectives. The Peer Kudos program allows employees to nominate one of their peers, an individual or a team, for recognition of a job well done. The nomination can be for anything that is viewed as going above an employee's regular job description. The submissions are completely anonymous and announced throughout the quarter.



DSS Leadership Advisory Board:

Forging the future for DSS leadership development

by Larry Cunningham
DSS Office of Innovation

During the January 2015 town hall, DSS Director Stan Sims addressed the challenges faced during 2014, and identified the opportunities that 2015 brings, to include the DSS Leadership Development Program.

Sims noted the DSS Leadership Development Program is one of his top priorities and he had dedicated resources for this initiative. He also endorsed the creation of the DSS Leadership Advisory Board (LAB) to serve as advisors on leadership development. The LAB consists of 11 members drawn from across the agency.

The LAB first met in December 2014 to participate in a DSS Office of Innovation workshop. Sims opened the workshop with a discussion on leadership and his expectations for the program. He emphasized that DSS leaders should be familiar with his "11 Principles" on leadership, which are:

1. **Know yourself and seek self-improvement**
   - Keep your strengths; improve your weaknesses
2. **Be technically proficient**
   - Know your duties and responsibilities, as well as those of your team members
   - Leaders don't do what their subordinates are capable of doing — train them
3. **Seek responsibility and take responsibility for your actions**
   - Grow, seek new challenges; accept consequences of decisions
   - Hold leaders accountable for performance of their subordinates (good/bad)
4. **Make sound and timely decisions**
   - Explore your options; decide quickly on a course of action

5. **Set the example**
    - Be a role model; leaders are on parade 24 hours a day
6. **Know your personnel and look out for their well being**
    - Earn your worker's trust; they will willingly accomplish the mission
    - Hold leaders responsible for training and developing their personnel
7. **Keep your followers informed**
    - Communicate; information encourages initiative, improves teamwork, enhances morale
8. **Develop a sense of responsibility in your followers**
    - Delegate; it will empower your people
9. **Ensure each task is understood, supervised and accomplished**
    - Provide clear expectations
    - Counsel your subordinates in writing when they don't meet these expectations to help them succeed
10. **Build a team**
11. **Employ your team in accordance with its capabilities**
    - Use sound judgment; failure is not an option

Sims also reminded LAB members that "it's all about our people." He expected the LAB to "forge the future ... that what the LAB was doing was on par with the most important thing you'll ever do for DSS ... today and for the future." He then provided his intent for the program:

- Identify emerging leaders
- Educate, train, and develop those we have entrusted with leadership responsibility and authority
- Provide the training, tools, and resources to those already serving, and develop those who will lead DSS in the future
- Produce caring, credible, accountable DSS leaders capable of motivating their employees and teams to be successful at achieving results that address the challenges of the national security environment

The LAB members were provided roles that included:

- Refine the DSS leadership strategy with a roadmap
- Create timelines and measures
- Link leader and individual development to DSS mission, strategy, vision, and goals
- Sponsor and oversee the Leadership Development program

More specific instructions outlined goals the LAB members must achieve, to include:

- Build a leadership development pipeline,
- Cultivate a leadership culture throughout the agency that exemplifies the competencies expected and demanded from leaders, and
- Provide education, training, and development opportunities for those who want to lead and those who do lead.

"With direction from the Director, the Leadership Advisory Board ... is working to create a DSS Leadership Development Program geared toward educating, training, and developing the next generation leaders needed in DSS and DoD."

Following Sims' remarks, the DSS Office of Innovation led the LAB members through a series of collaborative activities to analyze complex problems and produce rapid results.

The expected deliverables from the workshop were: Create a DSS LAB charter; establish criteria to identify emerging leaders; develop an organizational blueprint for educating, training, and developing DSS leaders; and cultivate a leadership culture throughout the agency. A charter has since been drafted and is in coordination with DSS senior leadership. In addition to the draft charter, the LAB members developed an action plan identifying eight steps the LAB must take in the development of a DSS Leadership Development Program. These included:

1. Define the outcomes of the DSS Leadership Development Program
2. Define and prioritize the target audience
3. Determine competencies — SWOT (Strengths/weaknesses/opportunities/threats) analysis
4. Identify best practices (government and industry)
5. Identify current DSS approaches
6. Re-evaluate the outcomes
7. Define delivery options
8. Identify DSS organizational constraints

With direction from the Director, the Leadership Advisory Board established a unified approach for achieving its intended goals and objectives, and is working to create a DSS Leadership Development Program, geared toward educating, training, and developing the next generation leaders needed in DSS and DoD.

DSS Welcomes ...

New IO Director

Gus Greene is the director, Industrial Security Field Operations. He is a member of the Defense Intelligence Senior Executive Service, and a retired U. S. Army officer with over 37 years combined service as an intelligence professional. Before joining DSS In March 2015, Greene served as the Chief of Staff for the Director for Defense Intelligence (Intelligence & Security) within the Office of the Under Secretary of Defense for Intelligence (OUSD(I)). During the period September 2007 to July 2013, Greene served in several positions within OUSD(I) to include Senior Advisor to Warfighter Support directorate; Deputy Director, Warfighter Support directorate; Director of Sensitive Activities directorate; and Assistant to the Deputy Under Secretary of Defense for Intelligence and Security.

A retired Army colonel with 27 years of distinguished military service, Greene also served in a variety of intelligence, operations, command, and staff positions from the tactical to the strategic levels including commanding a U.S. Army Intelligence and Security Command Brigade.

New IP Director

Fred W. Gortler III is the director, Industrial Policy and Programs. He is a Defense Intelligence Senior Level executive and a retired U.S. Air Force officer. Prior to joining DSS in May 2015, Gortler was the principal advisor for Intelligence Integration at the National Ground Intelligence Center, where he led U.S. Army efforts to integrate all-source analysis with customers and partners in the joint, interagency, intergovernmental, and multinational arenas.

Before this, Gortler simultaneously served the Director of National Intelligence and Under Secretary of Defense for Intelligence as the Director of Military Partnerships. In these roles, he helped implement the Intelligence Reform and Terrorism Prevention Act, executing the national vision for integrating national and military intelligence.

He is a retired U.S. Air Force colonel, and his last assignment was as the commander, 70th Intelligence Wing, Fort George G. Meade, Md. During his military career, he completed 14 Department of Defense and Intelligence Community assignments, commanding at the flight, detachment, squadron, group, and wing levels.

New Chief Information Officer

Craig E. Kaucher, a Defense Intelligence Senior Level executive, is the DSS Chief Information Officer. Prior to joining DSS, Kaucher served as the first Chief Information and Technology Officer for the Defense Media Activity (DMA). His focus areas and priorities were to improve the standardization and effectiveness of the technology architecture across DMA, improve and create more efficient technology acquisition practices, and to strengthen the information security posture of the organization. From June 2004 to June 2009, he served as the Director for Information Sharing and Knowledge Management, and CIO in the Office of Intelligence and Analysis, Department of Homeland Security. He was the founding government employee of this division and of the CIO function in this organization.

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

New Designated Approving Authority

Karl Hellmann is the DSS headquarters Designated Approving Authority. Before this, he served as the Regional Director of the Western Region. He began his federal service in 2006 as an Information Systems Security Professional with DSS in Chantilly, Va. In this position, he was responsible for reviewing and implementing established DoD policy regarding industrial security procedures, systems, standards, and regulations governing the safeguarding of classified information on information systems utilized by contractors in the National Industrial Security Program (NISP).

In July 2007, Hellmann was appointed acting Regional Designated Approval Authority (RDAA) for the National Capital Region, and in October, he was selected as the RDAA. In this position, he led a team in support of certification and accreditation of industry classified systems as well as subsequent annual assessments. He served as the Designated Approving Authority for the NISP on government contractor information systems within boundaries prescribed in the RDAA appointment letter.

Inaugural DSS Industry Day and Technology Exposition held at RKB

More than 300 people attended the inaugural DSS Industry Day and Technology Exposition, held April 8, 2015, in the Russell-Knox Building.

The theme for the event, hosted by the Office of the Chief Information Officer, was "Strengthening Partnerships to Achieve the DSS Mission." Approximately 38 companies participated in the technology exhibition.

The event provided an opportunity for industry to hear presentations from agency senior leadership on DSS' current initiatives and emerging challenges in the context of the changing technology and security environment as they related to the event theme.

"We are wholly reliant on industry for our technical capabilities, and therefore our success is dependent on industry understanding us very well," said Craig Kaucher, DSS Chief Information Officer. "That's what this day was all about."

While attendees were participating in the Industry Day sessions, the Technology Exposition was open for people to visit, network, and view demonstrations of the latest products and services from the participating industry exhibitors.

"Our first DSS Industry Day was a hugely successful event not only for DSS, but for our government partners at the Russell-Knox complex, and for our industry partners," said Kaucher. "In bringing together this unique intelligence and security-focused community with our industry partners, we were able to expand each other's knowledge of our needs and our strategic direction, as well as establish relationships for the future."

"In bringing together this unique intelligence and security-focused community with our industry partners, we were able to expand each other's knowledge of our needs and our strategic direction, as well as establish relationships for the future."

ABOVE, FROM LEFT: Chris Bowman, Office of the Chief Information Officer (OCIO), speaks with a vendor in the technology expo at the Russell-Knox Building on April 8, 2015. (Center) Craig Kaucher, the new DSS Chief Information Officer, answers questions during DSS Industry Day. (Right) Marcus Evans, OCIO, also speaks with a vendor at the expo.

Data Center Operations manages all digital tools, supports DSS employees

Say "data center operations" and most people imagine sterile, climate-controlled rooms housing row after row of server racks glowing with green and amber lights. While there's some accuracy in that vision, the "DCO is all about managing systems that just happen to reside on servers," said Eric Corbin, the DCO branch chief from the Office of the Chief Information Officer.

With over 700 devices supporting virtually every digital tool used by the employees of DSS, the work of the DCO is conducted in the 18,000 square-foot shared data center in the Russell-Knox Building and in Data Center West. These two facilities host four independent data centers, to include NIPRNet production, SIPRNet production, and pre-production.

Pre-production is where DCO stages pre-deployment systems and services before launching them live and where new code and patches are tested to ensure they are ready for primetime. It's also the alternate site that makes it possible for DSS to continue critical operations in the event of an outage or disaster at headquarters.

In its day-to-day work, DCO's core services focus on enterprise virtualization, collaboration services (Outlook, Blackberry, SharePoint, Lync), enterprise storage, enterprise database services, disaster recovery, application support, web services, backing up and restoring data, and management and monitoring of all the underlying equipment that makes these services possible. Concurrently, the 10-member DCO team is deploying enhancements and new functionality, with the support of Information Technology Systems Support (ITSS).

In support of new or enhanced applications, DCO integrates closely with other OCIO offices, to include Information Assurance, Network and Telecommunications Operations, and Computer Network Defense. Working together, these teams ensure systems are built, validated, secured, deployed, and maintained throughout the system development lifecycle.

Much like the power company, which people don't think about until there's an outage, DCO often measures its success through transparency. "I wouldn't say we labor in obscurity, but it's practically a job requirement to fly under the radar most days," said David Hobbs, DCO team lead and senior systems engineer. "If we're visible, it's probably because something is down." As an example, the team points to its 99.8 percent scheduled-uptime metric for exchange and Blackberry services in 2014 as an indicator of its success as a branch.

The DCO also measures its successes by the new services and capabilities it offers. Asked what he takes most pride in, Corbin praised the efforts of his team and the creation of Data Center West, the agency's disaster recovery site. The data center was built in June 2012 and its capabilities to provide redundant services in the event of outages or disaster are constantly expanding.

Additionally, the work of the DCO was key in the deployment and maintenance of instant messaging software Microsoft Lync (supporting over 30,000 instant messages weekly) and web platform software SharePoint (supporting over 140,000 web page views weekly).

Less visible to customers was the deployment of several monitoring tools, allowing the agency responsiveness to evolve from primarily reactionary to primarily proactive. In short, the branch is more capable of anticipating issues with systems and services, and responding before those issues impact the customer.

Currently, the DCO is closely integrating with OCIO Program Integration and Test and Evaluation offices in supporting other systems, to include the deployment of single-sign-on for National Industrial Security Program Central Access Information Security System, and the National Industrial Security System.

For the future, the DCO is assessing new technology to support the agency mission. This summer, the DCO will focus on migrating to Defense Information Systems Agency Enterprise Email. The branch has also piloted a smart device program, and is assessing DISA MilCloud as an option for the development and hosting of both existing systems and those that will deploy in the future.

DSS office dedicated to promoting small business opportunities

John Baumert, DSS Office of Acquisitions, became the DSS Small Business Specialist in December 2014. Here he provides an update on the small business program at DSS.

What is your role in relation to the DSS small business program?

As the DSS Small Business Specialist, I review all solicitations over $10,000 to determine if the requirement should be set aside for small businesses. I am the point of contact with small businesses to discuss how to do business with DSS. I am also available to assist in market research to look for small businesses that can work on DSS requirements.

How long has DSS had a small business program? Why was it established?

The DSS Office of Acquisitions was established at the start of FY09. For the first few years, DSS did not have a small business program, but the Office of Acquisitions tracked the percentage of dollars obligated to small businesses against the overall Department of Defense goals. The DoD Office of Small Business Programs assigned goals to DSS starting in FY11. The Small Business Act and the National Defense Authorization Act both require each agency with contracting authority to establish an office dedicated to promoting small businesses.

Has DoD set a percentage of competitively awarded dollars that need to be awarded to small businesses? If so, how is DSS doing? Or done in the past?

For FY14 and FY15 the DSS goal has been set at 50 percent. That means 50 percent of all dollars obligated on contract each fiscal year are required to go to small businesses. Through the first five months of FY15, our agency is just over 41 percent. However as an agency, we haven't obligated many dollars on contracts so far. DSS was able to meet its goals in FY11 and FY14.

What is DSS doing to increase the percentage of competitively awarded opportunities to small businesses? (i.e., outreach events, communications, etc.)

Communication with the small business community is important in meeting the DSS goal. In the past I participated in multiple events

where I was able to meet many small business firms. I participated in the DSS Technical Expo at the Russell-Knox Building in April 2015, where I gave a presentation on the DSS Small Business Program. I also field telephone calls answering questions and meet with small business firms upon request.

In your communication efforts, do you find that many small businesses are unaware of opportunities at DSS? Or don't know how to get into the DoD marketplace?

For the most part, no. Small businesses are aware of our agency and where the Office of Acquisitions posts solicitations of DSS requirements. My interaction with them is more on the types of requirements DSS has coming in the near future and for them to let DSS know they are an interested vendor in those requirements.

In the past, have any of your jobs had you interacting/working with small businesses? What advantages do they bring to the marketplace?

As a contract specialist and warranted contracting officer for the past 15 years, I worked constantly with the small business community. Small businesses are great for the economy and bring a lot of new ideas and innovative approaches to solving the government's requirements.

Instructional system designers at center of product development

by Erika Ragonese
Center for Development of Security Excellence

The creation of instructional products involves the efforts and talents of many people at the Center for Development of Security Excellence (CDSE). A team of curriculum managers, instructors, instructional system designers (ISDs), multimedia specialists, and courseware programmers is required in the development and delivery of instructional products.

Each part of the team plays a critical role: Curriculum managers offer the vision and direct product development, instructors leverage subject matter expertise, ISDs provide expertise in the instructional methodologies and process, multimedia specialists create visual and audio products, and courseware developers program eLearning products. But the ISD is at the center of the process, working with all other team members to facilitate the vision.

Responsibilities

CDSE's ISDs are key players in the instructional development process. They advise the curriculum managers and instructors on learning and instructional theories related to the analysis, design, development, implementation, and evaluation of instructional materials. They recommend options for instructional delivery approaches and learning activities that are best suited for the target audience.

ISDs also help develop learning outcomes and objectives, and provide advice on various student learning styles. They document the design for a product like an architect does for a house.

In addition, they help evaluate the effectiveness of instructional/educational programs, to include developing performance tests and questionnaires, and determining reliability and validity of evaluation instruments to ensure products are instructionally sound.

Skill Sets

The ISDs apply organizational, analytical, and creative abilities developed through formal education and professional experience. CDSE ISDs have experience working and/or serving in the military, government, industry, or even educational institutions.

ISDs develop various products and performance support tools such as eLearning, instructor-led, and education-level courses. They also develop the videos, job aids, and webinars created specifically for the security workforce. They use a systematic instructional development process known as the ADDIE model to create these products.

The ADDIE model is a five phase process, and ISDs play a critical part in each of the five phases at CDSE. ADDIE provides a structured and proven process to develop effective training, and ISDs also use this process to sustain CDSE products.

CDSE is able to support the security community's readiness through education, training, and certification as a result of the successful collaborative efforts of ISDs.

*(**Editor's Note:** Stephen Fowler and Samantha Dambach contributed to this article.)*

ISDs support the ADDIE process:

A In the Analysis phase, ISDs help the curriculum manager identify a learning solution, the target audience, course outcomes, delivery options, learning constraints, pedagogical approaches, and timelines for project completion.

D In the Design phase, ISDs use the vision (developed in collaboration with curriculum managers, instructors, subject matter experts, and courseware developers) to develop the design documentation (course framework) to guide the course development process. In the eLearning design process, ISDs create storyboards that provide a detailed roadmap to the course developer; it explains text, audio, and graphic requirements for programming.

D In the Development phase, ISDs coordinate with the course developers to ensure the design vision and specifications are reflected in the final product. ISDs assist in developing exams, arranging creative services support, and preparing administrative documentation, such as course descriptions and course management guides.

I In the Implementation phase, ISDs assist the course managers and instructors with the integration of the product into the curriculum and testing the product with students to ensure the product is instructionally sound prior to release or provide support in evaluating test results.

E Finally, in the Evaluation phase, ISDs help to develop surveys, evaluate results, and provide recommendations for improving the instructional product.

"Organized" and "Existing"

by Helencia Hines
Industrial Policy and Programs

One of the criteria for a company to be considered for a facility clearance is for the company to be "organized" and "existing" under the laws of any of the 50 states, the District of Columbia or Puerto Rico, and be located in the United States or its territorial areas in accordance with National Industrial Security Program Operating Manual (NISPOM) paragraph 2-102 b.

The NISPOM defines the United States and its Territorial Areas as the 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, Wake Islands, Johnston Atoll, Kingman Reef, Palmyra Atoll, Baker Islands, Navassa Island, and Northern Mariana Islands.

Industrial Security Letter (ISL) 2009-02 advises that for the purposes of NISPOM paragraph 2-102b, DSS will consider requests for Facility Clearances in only the "organized" United States territories of Guam, Northern Mariana Islands, Puerto Rico and the U.S. Virgin Islands.

On January 17, 2013, ISL 2013-01 was issued which provided clarification to NISPOM 2-201b that American Indian and Alaska Native Nations located within the United States, and recognized by the Department of Interior in accordance with Industrial Security Letter, ISL-2013-01, may also create companies that are eligible to be processed for facility clearances.

For companies to be "organized," they must be formed under a legally recognized set of operating doctrine such as Articles of Incorporation, Articles of Formation, Articles or Certificate of Organization, Partnership Agreement, Joint Venture Agreement, Federal or State Charter, etc., establishing its legal existence. In addition to a company's legal existence, DSS also requires a physical presence that it can go to and conduct security vulnerability assessments in accordance with NISPOM paragraph 1-206.

The NISPOM defines a facility as a plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. For purposes of industrial security, the term does not include Government installations.

Historically, the Unites States purchased or managed the territories in Trust on behalf of the League of Nations or United Nations mandates as a result of prior wars such as the Spanish American War, World War I and World War II.

In most cases the U.S. territories were managed by the U.S. Navy and then transferred to the Department of Interior, Office of Insular Affairs and/or U.S. Fish and Wildlife Service, as directed in Executive Order 11021 — "Administration of the Trust Territory of the Pacific Islands by the Secretary of the Interior." The United States categorizes its territories as either "Incorporated Territories" or "Unincorporated Territories."

Incorporated territories are those in which the United States Constitution is fully applicable. It has been held that individuals born in incorporated territories, can claim United States Citizenship under the 14th Amendment. Unincorporated territories and/or outlying possessions are areas in which the U.S. Constitution has not been expressly and fully extended by the Congress within the means of Article IV, Section 3 of the Constitution.

In essence, Congress must pass an act or law specifically authorizing U.S. Citizenship for citizens of unincorporated territories, otherwise individuals are designated as U.S. Nationals.

Territories are also either "Organized" or "Unorganized." Organized territories normally have an Organic Act issued by Congress establishing a civil government or there are a series of Acts formally establishing a civil government.

United States "Organized" Areas and Territories	Number of Facilities in the National Industrial Security Program
District of Columbia	290
Guam	3
Commonwealth of Puerto Rico	1
U.S. Virgin Islands	0
Commonwealth of the Northern Mariana Islands	0

Current security issues and threats presented at joint event

by Beth Alber
Office of Public and Legislative Affairs

In late March 2015, the Joint Industrial Security Awareness Council (JISAC) held its 19th annual seminar in Leesburg, Va., and was attended by more than 700 industry security personnel.

Guest speakers for the event included DSS Director Stan Sims; Retired Air Force Gen. Michael Hayden, former director of the National Security Agency; Randall Coleman, assistant director, Counterintelligence division, Federal Bureau of Investigation; and Valerie Heil, Security Policy and Oversight, Under Secretary of Defense for Intelligence. Hayden, who spoke at last year's conference, provided the group an update on advances in cyber security. He noted that industry/private sector has the primary role in cyber security and the government should play a supporting role. Government should work to enable industry in this role. Other presentations focused on a variety of issues, to include cyber security, insider threat, mitigating the risk of social media, and recent policy changes.

Additionally, the event featured a director's panel comprised of DSS mission directors — James Kren, Deputy Director; Bill Stephens, Counterintelligence; Kevin Jones, Center for Development of Security Excellence; Michael Halter and Heather Green, Industrial Security Field Operations; and Keith Minard, Industrial Policy and Programs. The panel provided updates on their respective areas, and then took questions from the audience, ranging from the status of ODAA Business Management System to publicizing the top 10 vulnerabilities in the Voice of Industry newsletter to developing an approved curriculum for school career days.

The JISAC was formed to assist defense contractors in complying with the requirements of the National Industrial Security Program. The council, comprised of both DSS representatives and industry personnel, demonstrates the continued partnership the agency is forging with industry. DSS employees serving on the JISAC include Emily Helstowski, JISAC co-chairperson and industrial security specialist, DSS Headquarters IO; Rod Webb, senior industrial security specialist, and Elizabeth Kim and Andre Jenkins, industrial security specialists, Chantilly Field Office; Robin Nickel and Shelton Mallow, industrial security specialists, Alexandria Field Office; Kevin Williamson, industrial security specialist, Hanover Field office; and Ursula Stearns, FOCI Operations Division.

The JISAC sponsors an annual joint event where security professionals from regional industrial security awareness councils, defense contractors and DSS industrial security representatives can gather and meet to share information on current security issues. The collaboration by JISAC helps promote the protection of classified and proprietary information through increased awareness programs, training, and the distribution of security awareness materials.

Members of the Montford Point Marines recall personal experiences of their time at Camp Montford Point, N.C.

Celebrating Black History, life and culture

As part of the 2015 Black History Month celebration, DSS headquarters hosted Congressional Gold Medal recipients, Montford Point Marines in February 2015.

The theme for the celebration was "Black Life, History & Culture," and the program featured personal accounts of the four Montford Point Marines in attendance — Retired Master Gunnery Sgt. Carrol Braxton; retired Gunnery Sgt. Richard H. Walker; retired Staff Sgt. Johnny B. Cody; and retired Private First Class Stanley Tapscott.

These four retired Marines received basic training at the segregated Camp Montford Point in Jacksonville, N.C., following President Franklin Delano Roosevelt's effort to erase discrimination in the military.

Their stories brought to life the challenges faced by Black recruits during that timeframe. Additionally, the "DSS Voices" provided a musical selection during the celebration.

Ensure security isn't seen as a roadblock, rather an integral part of work

In March 2015, Dr. Mark Lowenthal, a former employee of the Central Intelligence Agency and president of a national security education, training and consulting company, presented "Secret and Security — post Snowden," during a Human Capital Management Office Lunch-N-Learn program.

Lowenthal referred to Edward Snowden as a "leaker, not a whistleblower" and discussed the ramifications of his actions on secrecy and security in today's environment. "There is risk," he said. "This is a risk-based business; we are never going to eliminate risk completely."

However, "when you think about how many people are currently working in DoD and in industry, and the relatively few mishaps we've had, it's pretty impressive," he said. "DSS is in a tough spot, but you've got to keep up the messaging and be sure that security is not seen as a roadblock, but as an integral part of what people must do to protect themselves and their work."

Lowenthal also attended the agency's Senior Leader Annual Meeting and helped kicked off the event with "Some Thoughts on Leadership." His presentation echoed many of the themes from the three-day event and reminded the leadership team that people are an organization's best and most important resource.

As a result, he encouraged the team to take an inventory of themselves as leaders and spend more time focusing on people and letting them do their jobs.

Running marathons in remembrance

DSS employees and family members recently participated in two marathons, both with tragic histories.

On April 20, Brian Murphy, senior action officer in the Irving Field Office, and his wife Lisa, ran in the 2015 Oklahoma City Memorial Marathon.

More than 25,000 people ran the marathon, which was held in conjunction with a remembrance ceremony recognizing the 20th anniversary of the Alfred P. Murrah Federal Building bombing in 1995, which killed 168 people to include five Defense Investigative Service employees.

"This being the 20th anniversary, the tributes were very moving including battalions of fire fighters marching along with the runners in their full turnout gear," said Murphy.

Also on April 20, the wife of Philadelphia Field Office Senior Industrial Security Representative Steve Eisenberger ran in the 119th Boston Marathon. Susan Eisenberger, who battled a strong headwind for the majority of the run, finished with the race in 4:16:30.

"We loved Boston, and it was an experience we will never forget," said Susan. "Every person watches the marathon as a fan — they are amazing; they give you faith in hope and kindness."

Brian Murphy and his wife Lisa after completing the 2015 Oklahoma City Memorial Marathon.

(Left) Jake and (right) Steve Eisenberger cheer on wife/mother Susan before the running of the 119th Boston Marathon.

Defense Security Service