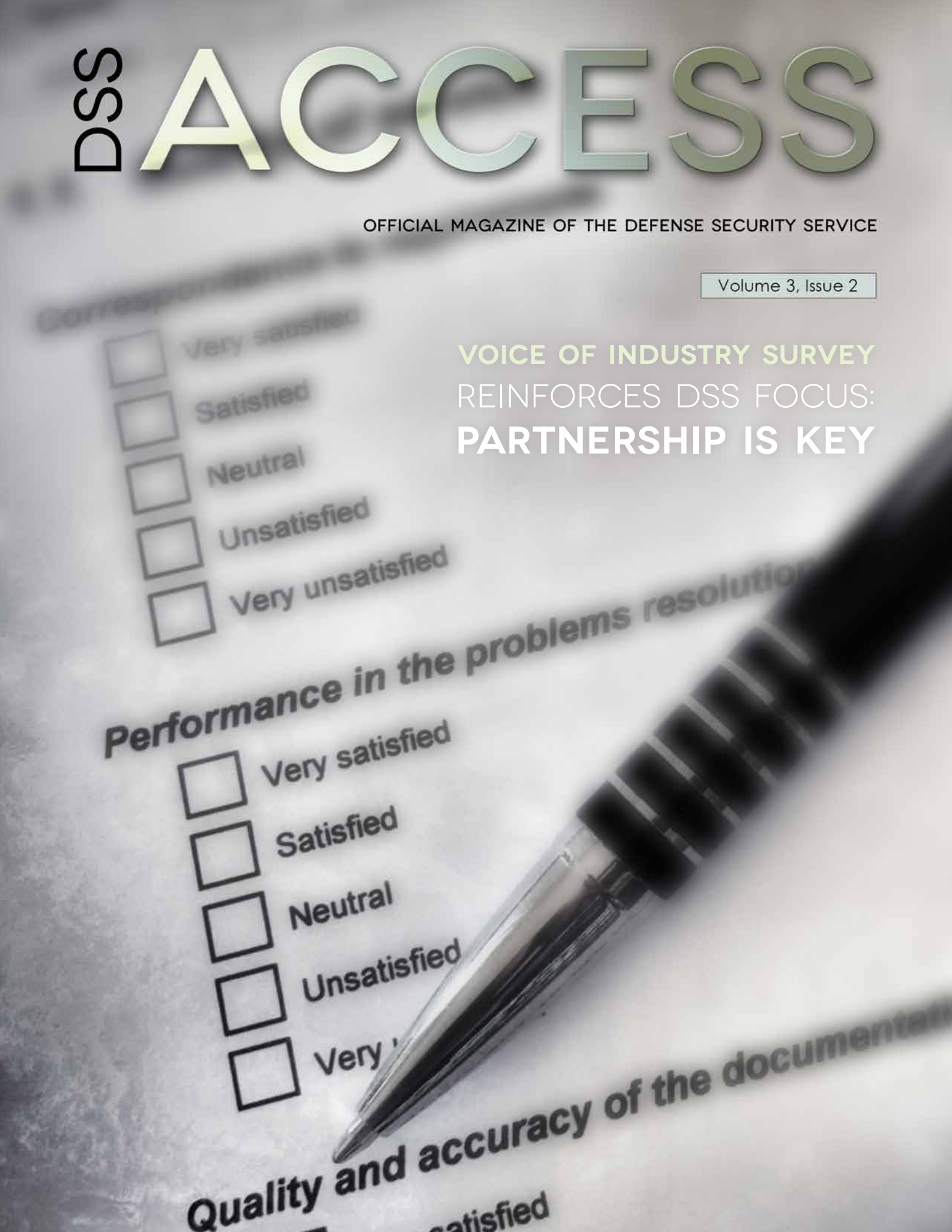
DSS ACCESS

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE

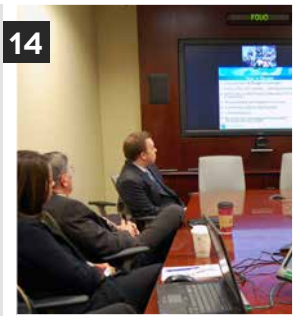
Volume 3, Issue 2

VOICE OF INDUSTRY SURVEY REINFORCES DSS FOCUS: PARTNERSHIP IS KEY



SUMMER 2014

Volume 3, 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

Chief of Staff
Rebecca J. Allen

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

Anyone who reads these pages knows the emphasis I place on our relationship with industry. The cover story of this issue, our annual Voice of Industry survey, demonstrates that commitment and the benefits it delivers.

We see a direct correlation between our engagements with industry and the level of satisfaction reported. Instead of keeping DSS at arm's length, our industry partners would like to see more of us!! I don't think there are many oversight or compliance agencies in the government that can say the same. I want to thank all those who responded to our survey. We do read the responses, and we value the feedback we receive.

As I stated at our town hall meetings earlier this year, I laid out my vision when I came to DSS, but the men and women of DSS executed it. Our personnel have embraced the change, and you can see that in many of the articles in this issue.

The annual Foreign Ownership Control or Influence Conference has been extended to a second day to reach key facility security officers. Our Triage Outreach Program focuses on smaller facilities that may not have full-time security staff. Our Personnel Security Management Office – Industry, is actively engaged in webinars and other venues to make sure industry is aware of how changes in policy or procedures affect them. And our team at the Center for Development of Security Excellence developed the FSO Toolkit, which puts the critical information an FSO needs at their fingertips. These examples exhibit our commitment to partnership and ensuring industry has the tools and information they need to be successful.

I am very proud of our accomplishments these past three years, and I am optimistic and excited about our future.

VOICE OF INDUSTRY SURVEY REINFORCES DSS FOCUS:

PARTNERSHIP IS KEY

By Ryan Deloney, *Industrial Security Field Operations*

Based on responses to the 2013 Voice of Industry (VOI) Survey, DSS' partnership with industry is stronger than ever. Overall, the level of satisfaction with DSS remained consistent, as 95 percent of Facility Security Officers (FSOs) responded positively to overall satisfaction with the guidance and support they receive from DSS.

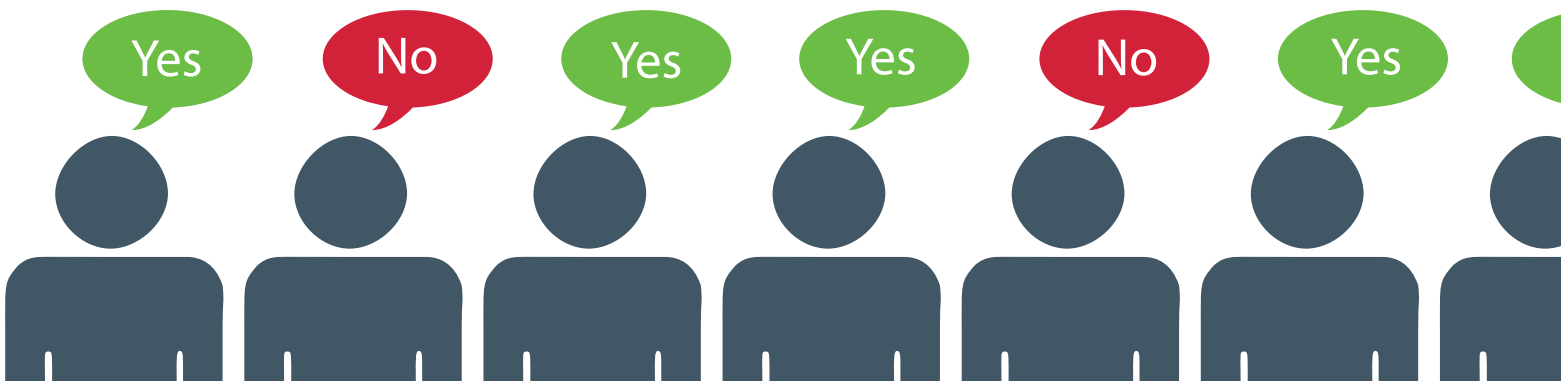
DSS launched its third annual VOI Survey in October 2013 to solicit feedback from U.S. cleared defense industry on the agency's performance with respect to the administration and implementation of the National Industrial Security Program (NISP).

The survey, which was open for four weeks, was sent to over 13,000 FSOs, with approximately 10,000, or 72 percent of participants responding. This mirrors response rates from previous years. Each section of the survey featured various multiple choice and open ended questions.

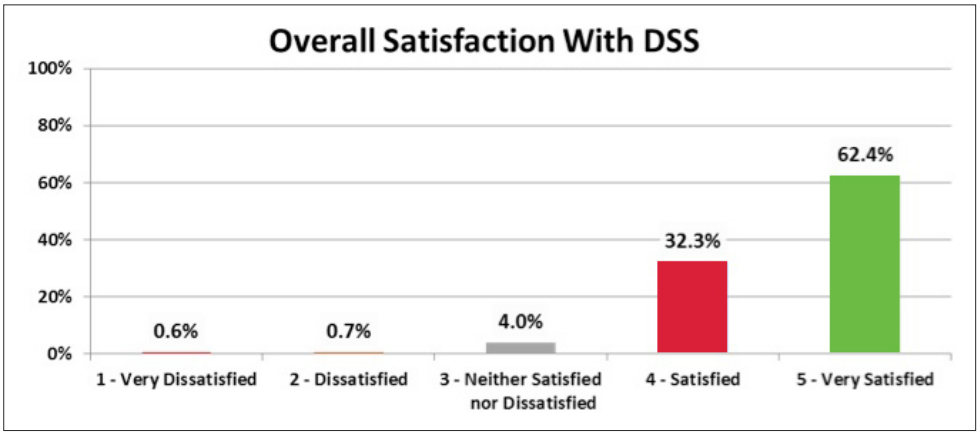
A key component of the survey is the analysis that DSS conducts to determine areas for improvement. For instance, in the industrial base, a large portion of FSOs have five to 15 years of experience in security. The largest, most complex sites are those with the most seasoned FSOs, while smaller possessors and non-possessors have the least experienced. DSS will continue to target training and education efforts to reach these smaller locations.

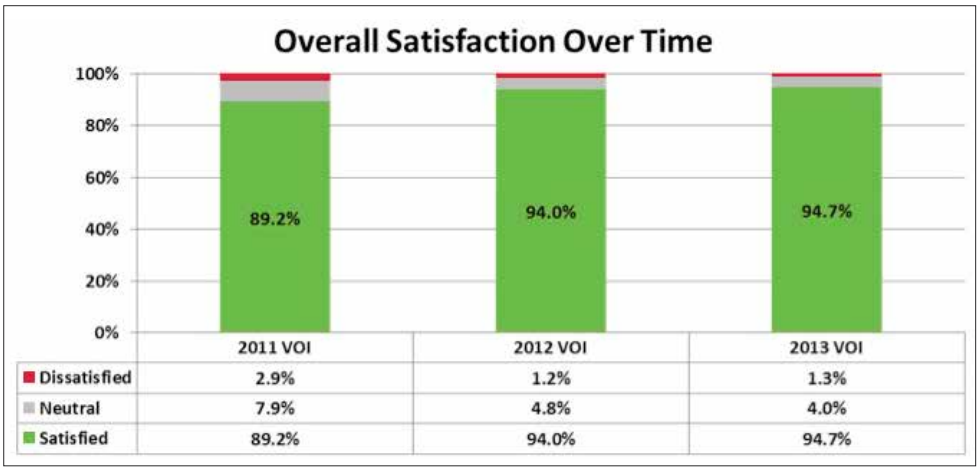
Some survey comments also highlighted many best practices that DSS will continue and seek to expand and standardize as appropriate:

- **"Participation in industry events. This demonstration and accessibility allows industry and government to form a better collaborative environment. In addition, questions and concerns can be addressed quickly."**
- **"Active partnerships. I am able to get support and information from him outside of our assessments, which helped further the training I was already required to take."**
- **"Actively supports communication with industry through once or twice a year 'Day with DSS' symposia."**
- **"My DSS rep helped me build a rough plan for our first year. This was so helpful and allowed us to start early building our security program to align with DSS best practices."**
- **"Monthly newsletters are very effective."**
- **"All our local DSS reps are very active engaging local law enforcement officials."**
- **"Annual open house meetings for FSOs to meet with DSS reps in their field offices."**
- **"Bring the Counterintelligence (CI) Representative with you as he/she can help in doing interviews such as those who have traveled overseas, not to mention the CI insight he/she can provide due to experience and expertise."**
- **"The webinar seminars/training are outstanding and would like to see even more of them."**
- **"Threat assessment emails related to cyber attacks are a great tool."**



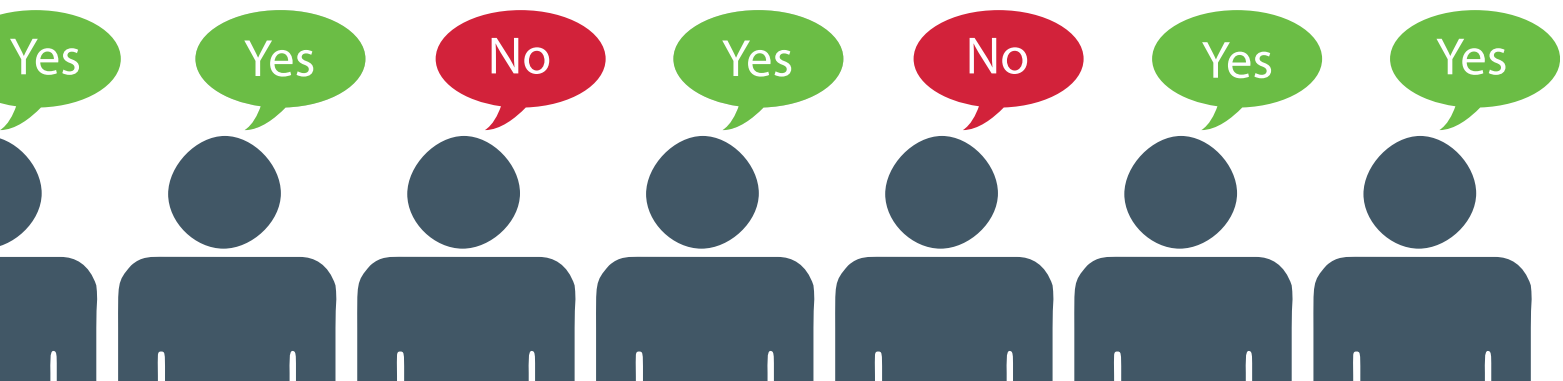
Compared to previous VOI surveys, 2013 had the highest positive rating!





When asked for recommendations, FSOs were very open with ideas on how DSS can improve:

- **"Would prefer that more attention is placed on cloud and mobile computing as it is a major source of concern for the protection of sensitive information. And this threat is expanding on a daily basis."**
- **"Please promote the importance of the FSO beyond that of an overhead job. FSOs need your support and encouragement from their management teams."**
- **"Would like DSS to consider breaking the James S. Cogswell Award into categories based on size and complexity of program."**
- **"Why isn't the National Industrial Security Program Operating Manual (NISPOM) updated to an electronic living document that can be updated as needed?"**
- **"We have seen a drastic increase in the use of sensitive but unclassified information. I would like to see DSS take on the role of standardizing this."**



- **"When implementing new security requirements, keep very small businesses in mind. Possibly offer alternative solutions for requirements that create financial hardships for very small companies."**
- **"Reporting on cyber issues is still a challenging area. The volume of attacks we get is massive, and we recommend some form of automation be used to report events to DSS."**
- **"Provide additional presentations that can be used for training (internal threat, International Traffic in Arms Regulation, Cyber Security)."**
- **"Combine JPAS, ISFD, etc. into one database."**
- **"A ticket tracking system for tracking open issues or inquiries. Email causes many issues to get lost in the volume. If a ticket system was implemented, an issue could be tracked from start to finish."**

Overall, DSS is highly regarded as the key partner with industry to provide core security oversight and assistance to protect classified information.

Frequency of interaction between field personnel and industry, specifically outside of the assessment cycle, builds stronger partnerships and openness of communications and directly links to improved assessment ratings.

DSS will continue to explore avenues to have more Industry touch points, i.e.: Field Office open house events, more participation in local industry organizations, recurring monthly emails, etc.

The next Voice of Industry Survey will be deployed in October 2014 and will include FSO feedback to streamline the submission form and focus on key areas.

This will reduce the time it takes to respond while still capturing critical information that will further improve the partnership between DSS and industry as we work together in our national security mission.

When asked what was perceived as the greatest threat to their program, FSOs highlighted cyber and insider threats as top concerns. DSS will continue to focus on these areas with industry and government partners.

When asked about one word that best describes DSS, the FSOs overwhelmingly recognized DSS as a helpful and professional partner in national security:

KEY FINDINGS

Very few FSOs (3 percent) had a decrease in satisfaction with DSS, while a third (35 percent) reported an increase in satisfaction.

Specific examples for enhanced satisfaction include:

"Team effort improved"

"Collaborative nature of meetings increased"

"Better explanations (i.e. assessment rating)"

"More proactive voice than reactive voice"

"The old joke about 'I'm from the government, and I'm here to help!' is not a joke anymore, it is perceived to be, and is in fact, a reality."

FSOs believe there is a true partnership with DSS (~ 90 percent).

Specific recommendations on how to improve partnership include:

"Continue with outreach"

"Decrease turnover"

"Build relationships outside of the assessment"

"More network security help"

"Work better with small business"

"Increase staff"

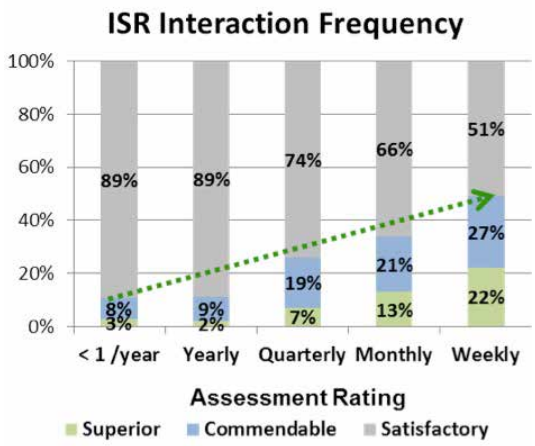
"Keep processes simple"

"Remain consistent"

"Participate in local industry group"

Increased interaction between an FSO and an Industrial Security Representative (ISR) was shown to have a direct impact on the Vulnerability Assessment ratings.

In fact, FSOs who interacted with their ISR more often than once a year are 2.3 to 4.5 times more likely to receive a "Commendable" or "Superior" rating.



FSOs recognized the high quality and value of the classified and unclassified threat products produced by DSS. Many had indicated they had not seen the unclassified products, which for reference can be accessed at www.dss.mil/isp/count_intell/ci_reports.html.

On the assessment side, respondents think the updated Assessment Rating Matrix is an effective tool, with 98 percent of facilities stating its ability to effectively rate security programs is "adequate" to "very good." Additionally, facilities feel that DSS is consistent with NISPOM requirements and processes, with 94 percent noting "often" to "always" consistent.

INNOVATION IS FOCUS OF

The third annual Director Awards ceremony was held in late March and recognized achievement, teamwork, accomplishment and innovation within individual offices and across the agency. In addition to awards for Employee and Team of the Year, this year a new award, Excellence in Innovation, was presented to a team.

In his opening remarks, Stan Sims, DSS Director, said the Director Awards program was near and dear to him, and he valued the opportunity to recognize those employees who go above and beyond to achieve results and get the job done. Sims also noted a recent article he had read on leadership and employee engagement and related it to the day's ceremony.

"The article said that employees who are engaged or highly committed to their work put their heart into what they do. They take pride in their work and look to make a difference. That's why we're here today," he said. "The employees we recognize today did just that. They set an example and inspire other employees to be more like them."

Sims added that there were many other DSS employees deserving of recognition and encouraged all employees to stay motivated and continue to demonstrate their capabilities. 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 2013 was Christine Beauregard, Security Specialist, Center for Development of Security Excellence (CDSE), who was nominated for leading the effort to launch the first electronic toolkit for Facility Security Officers (FSOs). The toolkit delivered critical access to information and training opportunities for the customer while saving travel costs.

As the driving force behind the development process, Beauregard single-handedly managed the collaboration with contractors, field offices, media services, and above all, the defense industrial base, the primary customer. As a web-based product, the FSO toolkit is available to anyone at any time, and saves time and money in the administration of security programs at over 13,000 cleared facilities. She reviewed over 350 security products, training aids, checklists, templates, references and other support material for inclusion in the toolkit.

Beauregard also piloted CDSE's prototype "Learn@ Lunch" series of industry webinars. This year she hosted or coordinated 12 webinars, which reached an audience of 5,500 attendees and celebrated a record attendance of over 800 in a single webinar.

Both initiatives concentrated on delivering critical access to information and training opportunities for the

ANNUAL AWARD CEREMONY

customer, while saving both industry and government agencies the costs of travel.

Finally, Beauregard was recognized for her customer focus and responsiveness to the needs of the community as she routinely receives critical feedback directly from the customer. Through this feedback, it was noted the Self-Inspection Handbook required modernization. After extensive collaboration, a new form was produced within two months.

The update to the Self-Inspection Handbook refreshed references and policy changes and improved upon the overall process. Within the first week of launch, the site was visited 2,342 times with 353 downloads.

In accepting the award Beauregard said she was humbled and honored by the award. "I am humbled by the people I work with at DSS; people who make the agency what it is. I am also humbled because there are so many deserving people at DSS. I'm honored because I had such an amazing opportunity to work on a project that affects so many people and I really feel like I've made a difference."

Also nominated for Employee of the Year were:

Jon Bennett, Congressional Affairs Specialist, Office of the Chief of Staff, was nominated for his responsiveness using extreme agility, professionalism, and competence to a number of highly visible, high value Congressional engagements. These engagements included interaction with Congressional members and their staffs, and delivering critical messaging regarding DSS involvement with several emerging national security priorities.

Francis Bonner, Intelligence Specialist, Counterintelligence, was nominated for his efforts, which led to 52 new investigations and/or operations during the year. This was the single highest number among the 51 field counterintelligence specialists in the CI directorate.

Nicholas Levasseur, Security Specialist, Industrial Security Field Operations, was nominated for developing, managing and sustaining strategic partnerships with industry and other government agencies to integrate improvements to service delivery, policy and processes.

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. This year's winner was the "SIPRNet [Secret Internet Protocol Router Network] to the Field" team.

"SIPRNet to the Field" was one of the agency's highest priorities and was a collaborative effort led and facilitated by Business Enterprise that delivered hard line SIPRNet installation to regional, field and resident offices. The team kicked off in January 2013, and identified 30 initial sites for SIPRNet upgrade. To date, 16 sites have been completed.

The team successfully minimized the impact to field work schedules and continued to keep field operations running smoothly during deployment. The hard line SIPRNet implementation saves the agency money by having SIPRNet traverse unclassified communication lines and included the installation of DS3 network lines. Using this method of accessing SIPRNet saves money in operating and maintaining the network and its associated peripheral devices.

In addition, Secret open storage allows for Counterintelligence analysts to streamline storage and presentation of classified data, as well as allowing their desktop computers to stay connected. New alarm systems and monitoring services now provide increased security to the remote sites, adding increased efficiency of operations.

The "SIPRNet to the Field" team extended to stakeholders from four different federal agencies: the General Services Administration, Defense Information Systems Agency, U.S. Army Corps of Engineers, and DSS. GSA and the Corps of Engineers, as leasing agents, managed and executed the renovation and

construction required to ensure compliance with standards for the open storage of classified information.

The "SIPRNet to the Field" team was comprised of representatives of multiple offices and disciplines working together. Since the inception of the project, the team has conducted extensive travel across DSS field offices to ensure all construction and technology upgrades were on budget and met the scheduled milestones.

In presenting the team award, Sims noted the size of the team, "It really shows this was a team effort, and I'm very proud of this team," he said. "SIPR to the field is so important for us to operate in a secure environment."

The "SIPRNet to the Field" team included the following members:

Office of the Chief Information Officer

Matthew Powell *(who accepted the team award)*

William Albach
Chris Bowman
Robert Carman
Marcus Evans
Paul Fox
Ron Harris
Greg Hensley
Bill Irvine
Joe Jackson
Delmar Kerr
Brad Lowitz
Ali Mohammed
Brian Padilla
Robert Riggle
John Urich
Mubarak Allotey
Willie Brokenburr
Aaron Doty
Mark Failer
Luis Garcia
Brian Hazuga
Dave Huntley
Barbara Jackson
Will Jolley
Matthew Kroelinger
Justin Milum
Kim Moore
Mardoqueo Perdomo
Julien Stephenson
JC Walker

Logistics Management Division

Michele Boldt
Lashawn Hazel
Randy Staples
Aster Gilmer
Matthew King
Steve Turner

Tom Xenakis

Industrial Security Field Operations

Gerald Curry
Selena Hutchinson

Counterintelligence

David Bauer

Financial Management

Sue Daniels

Office of Security

Ken Beckett
Tim Harrison
Angelo Reese

Office of Acquisitions

John Baumert

Office of Program Integration

Andy Branigan

Also nominated for Team of the Year were:

Command Cyber Readiness Inspection (CCRI) team, Industrial Security Field Operations, was nominated for enhanced oversight of SIPRNet sites in cleared industry.

International Division team, Industrial Policy and Programs, was nominated for preparing an innovative transition plan for non-adjudicative functions from the now disbanded Defense Industrial Security Clearance Office to the International branch. This plan improved procedures for DSS stakeholders and direct support of bi-lateral industrial security agreements with key U.S. allies.

Office of the Registrar team, CDSE, was nominated for understanding worldwide customers' needs, rising to every challenge in assisting customers within DoD and industry, and ensuring those executing security duties have the information to improve protection of missions supporting national security.

Excellence in Innovation of the Year

The Excellence in Innovation of the Year award is given 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 inaugural award was presented to the FSO Toolkit development team from CDSE. The FSO Toolkit was deployed in September 2013 and was the first in a series of planned toolkits. The award justification noted the development team demonstrated a "remarkable feat of originality, impact, and value as they produced an innovative prototype for access to security resources.

"In conjunction with customer feedback, the CDSE team recognized the process required for day-to-day operations as an FSO was inadequate and cumbersome. FSOs were traditionally isolated from resources and were left to their own devices to develop and manage an effective security program. Though resources were available from various organizations and venues, there was no single repository of critical tools required for an FSO to be successful.

In presenting the award, Sims emphasized many of these same points. "We just do not have the resources or capability to train every FSO at CDSE," he said. "So this team looked at other ways to reach these 13,000 plus security professionals. The result of their efforts is a tool that provides everything an FSO needs at the touch of a button. And industry loves this."

Most of the products contained within the FSO Toolkit were obtained through collaboration with Field Operations as well as various industry groups and organizations. This collaboration resulted in a peer-review process conducted by subject matter experts and incorporation of the latest products and resources, ensuring consistent and accurate information was included.

Conceptually the FSO Toolkit is simple, but employment of the concept had not effectively been accomplished before now. In its first three months, the FSO Toolkit was viewed over 40,000 times.

Team members of the FSO Toolkit are:

Christine Beauregard
Stephanie Crisalli
Peter DeCesare
Amanda Johnston
Renaye King
Stephen Raymond
Rojohn Soriano

Employee of the Quarter

Also recognized during the ceremony were the Employees of the Quarter for 2013:

Employee of the First Quarter: Nick LeVasseur, Personnel Security Management Office for Industry

Employee of the Second Quarter: Ronald Adams, Center for Development of Security Excellence

Employee of the Third Quarter: Wayne Chin, Industrial Policy and Programs

Employee of the Fourth Quarter: Maria Ong, Industrial Policy and Programs

A LOOK BACK AT SUCCESSES

DSS Director Stan Sims held two town hall meetings on Jan. 28, 2014 for agency employees. For the first time, the two sessions were available live to field personnel across the country using video teleconferencing technology installed in the past year. *(See related article on page 14.)* Each session had up to 25 remote sites connected and employees were able to ask questions using the agency's new instant messaging system.

In his opening remarks, Sims noted that this was his third agency townhall. Before looking back on 2013, Sims said he wanted to assess the progress the agency had made in the past three years and review the priorities he identified when he arrived — priorities that continue today:

1. **People first, mission always**
2. **Partner with industry**
3. **Tell the DSS story**

"We're a people business and we've accomplished a lot," Sims said. "We are a better organization than we were three years ago." He noted a reformed hiring process and the establishment of an employee recognition program as examples of efforts that benefit employees. "We are doing good stuff inside the agency that takes care of people," he said.

Sims described the agency's partnership with industry as the best it's ever been. He said, "We are a compliance organization and we have to ensure they're compliant. We're not easy or softies — we're still invalidating clearances, still issuing unsats [unsatisfactory security ratings], but we're doing it in a manner that is productive for national security," he continued. "The companies help us serve national security and there is trust, confidence and transparency with industry that we didn't have before."

Triage Outreach Program to contact cleared facilities that had not had a recent vulnerability assessment.

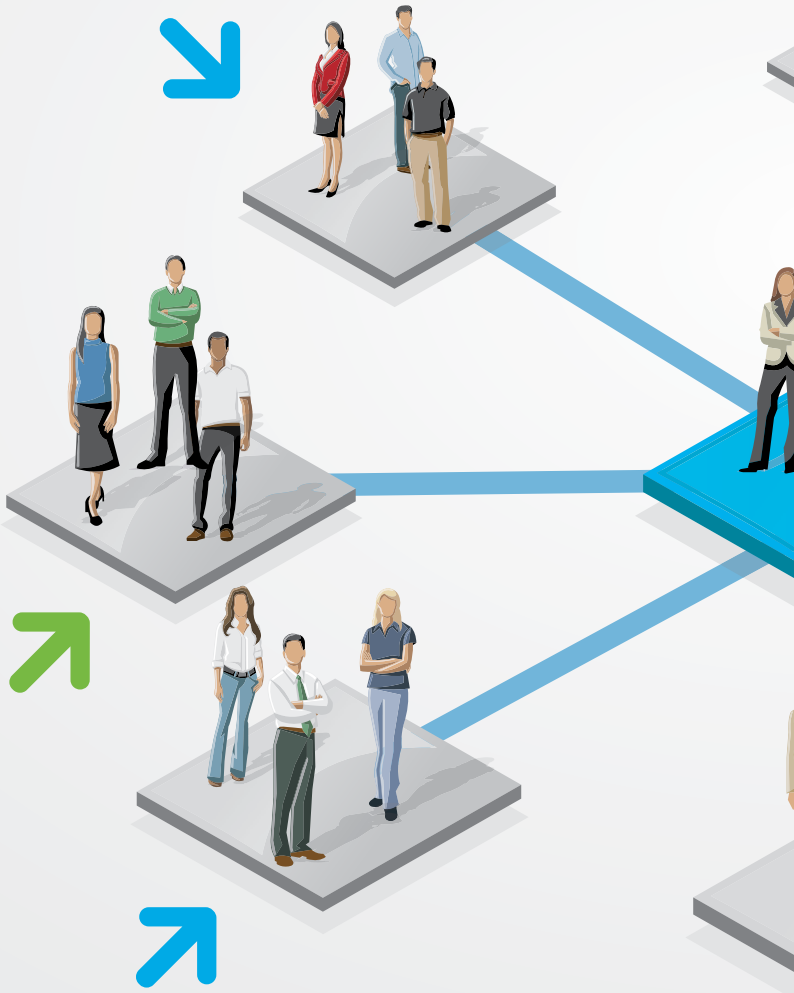
Sims said it was important to tell the DSS story because DSS is a small organization with few resources. He said decision makers and government stakeholders don't always understand why the DSS mission matters. "We need to let our colleagues know — within DoD and the federal government — why we matter. We have to explain how what we do is connected to what they do," he explained.

Sims concluded his overall assessment by stating, "This is not the same DSS as when I arrived. Thank you for seeing the vision I set and executing it. We've made tremendous progress but we will continue to move forward. I'm very proud of our accomplishments of last three years, but excited about the future."

Sims said that in spite of furloughs, the government shutdown and resource challenges, DSS continued to improve in 2013. "We've been resourceful and good stewards of the taxpayer's money," he said. "Everything we accomplished was done in spite of sequestration and budget challenges. We have to be efficient with our resources; think about what you're doing."

Sims then cited a number of accomplishments from the past year:

The agency's Wounded Warrior program, which leads the intelligence community in hiring Wounded Warriors and interns.



Command Cyber Readiness Inspections, which continued to transition to DSS from the Defense Information Systems Agency.

AND AHEAD TO CHALLENGES

Sims spoke at length about automation initiatives underway at DSS. "This is the research and development for the future that we're investing in today," he said. "We have not done a good job investing in the future, and we need to be masters of the information we already have."

Successes in Counterintelligence to include helping industry recognize threats to their technology.

Revised rating matrix for industry assessments which changed some enhancements and clarified others.

The National Industrial Security System (NISS) is the future system to replace the Industrial Security Facilities Database with the goal of automating more processes and building in metrics with data driven input from industry. The NISP Contract Classification System (NCCS) is designed to automate the DD Form 254 — the foundational document for classified contracts which remains a manual process.

Sims said there are challenges ahead for FY14 and that DSS is at the focal point of many changes the Department is working on — insider threat, personnel security, cyber operations, information sharing, CFIUS [Committee on Foreign Investment in the United States] and foreign ownership, control or influence.

Career mapping initiative to help employees chart a career path for the most common agency positions.

Liaison officer position established at the Office of the Under Secretary of Defense for Intelligence to connect with key leaders.

Sims noted a new Executive Order concerning insider threats and said DSS was taking it seriously with the goal of establishing a program to identify when employees were in trouble and provide help for them. "We want to prevent insiders from happening," he said.

DSS is well positioned to achieve audit readiness and Sims noted DSS was leading the Department. He also discussed a new leadership development program designed to pair with career mapping that will prepare employees for leadership positions. "We don't want leaders to fail because they didn't have the proper training," said Sims.

In closing the sessions, Sims said, "I want you to know we're in good shape with regard to our mission. Regardless of the budget and situation, we've done a great job with what we have. This is a total team effort to include all mission and support elements. We need support people to help us do our jobs and we need to thank them. Know who they are, recognize them, thank them. They are part of this team."

Governance process that instituted a three-pronged process to take decisions to the executive level.

INCREASED USE OF VIDEO TELECONFERENCING SAVES TRAVEL DOLLARS, TIME

With the restricted resources in today's fiscal environment, the Defense Security Service is foregoing travel and increasingly turning to video teleconferencing to communicate with its employees, stakeholders and industry partners. Video teleconferencing, or VTC, is a communication technology that permits users at two or more different locations to interact by creating a face-to-face meeting environment.

The VTC initiative began in late 2009, with installation of the infrastructure at DSS headquarters at Braddock Place in Alexandria, Va. The first region to receive VTC equipment, or an endpoint, was the Western Region. When DSS headquarters transferred to the Russell-Knox Building (RKB) at Quantico, the infrastructure was relocated to the RKB Data Center.

At the time, roughly 200 endpoints were available, but the VTC system was confined to users within the DSS network. By 2011, all DSS regional offices and most DSS field offices had operational VTC equipment.

In 2013, the VTC infrastructure was upgraded and provided the capability to communicate outside of the DSS network. Currently there are more than 250 endpoints running on the DSS unclassified network, and work has started on integrating the Microsoft Lync system with the VTC infrastructure, which will provide video and audio capabilities to all DSS employees.

Along the way, there have been challenges in setting up the VTC capability. Issues ranging from proper configuration of the

"The unclassified VTC is a great tool to complete the mission in our present resource-constrained environment."

Rich Hibbs
Field Office Chief, San Antonio

equipment so that the systems communicate correctly with each other, to using the proper Security Technical Implementation Guide requirement for a government network. All the lessons learned have been incorporated into the deployment of secure VTC capability. The first phase of SIPRNet VTC installation recently finished, with 30 sites online, and additional installations are planned over the next two years.

VTC came in handy for the San Antonio Field Office in conducting an initial Security Control Agreement meeting with an industry partner in early January 2014. The original plan was for a contingent from both the Southern Region Office in Irving, Texas, and San Antonio Field Office to travel to Houston, Texas for the meeting. This would have required six to nine hours of travel time round trip and travel funds for all participants. It also required a FOCI Operations Division action officer and a member of the Office of General Counsel to travel from Quantico, Va., to attend the meeting.

The field office and regional leadership discussed conducting the annual meeting using unclassified VTC and considered it a beta test for future meetings. The facility was included in the planning to ensure the technical compatibility of the VTC systems, and the DSS Office of the Chief Information Officer was brought into the discussions to gain insight and provide technological expertise.

Ultimately, due to inclement weather, the FOCI personnel were unable to travel. The VTC was conducted with the facility, and included both field and headquarters personnel with no technological issues noted.

"The unclassified VTC is a great tool to complete the mission in our present resource-constrained environment," said Rich Hibbs, field office chief of the San Antonio Field Office. "While some would argue that person-to-person interaction is always the most effective method, the use of unclassified VTC capabilities affords us an additional venue to communicate with our industry and government partners."

Another example of the technology's reach came in late January 2014, when DSS Director Stan Sims held two town halls in the RKB. While he gave his "State of the Agency" presentation to a packed room, the event was also streamed to more than 44 locations across the United States.

The event was held in two sessions to accommodate the size of the headquarters staff, and to allow employees in the east and west to watch at a reasonable time. Additionally, employees in the field and conference rooms across the headquarters had the option to submit questions directly to the townhall using the Microsoft Lync instant messaging system.

Ensuring the technology worked during the event was the responsibility of Luis Garcia, OCIO network manager, and his team, comprised of Adam McBride, Ken Diggs and Barry Turk. The team tested the system about a week in advance and coordinated with each location's administrative personnel to provide operating instructions and work out any issues.

A lesson learned after the event, Garcia noted, "We probably want to provide more information to the field offices on how to operate the VTC units so in the future we can minimize the bugs and minor issues."

ANNUAL CONFERENCE BRINGS FOCI COMMUNITY TOGETHER

By Stefanie McCabe
Industrial Policy and Programs

The Defense Security Service (DSS) held its annual Foreign Ownership, Control, or Influence (FOCI) Conference in April for companies operating under FOCI mitigation agreements. Approximately 350 Outside Directors, Proxy Holders, and Facility Security Officers (FSOs) attended. This annual event, held 18 times since 1989, was originally developed for Outside Directors and Proxy Holders of FOCI companies. In 2010, DSS hosted the first conference designed for FSOs of FOCI companies, and based on the initial feedback, DSS determined to make their involvement an annual event.

The conference raises awareness within the two communities of current DSS and FOCI-related concerns and issues. It also provides a forum for contractor input regarding the implementation of FOCI mitigation agreements and security oversight at FOCI facilities.

Opening Remarks

DSS Director Stan Sims opened both days by welcoming attendees and presenting an overview of the current state of DSS. He also discussed his vision for the future of the agency in light of the changing security/risk environment.

Due to recent events, such as the shooting at the Washington Navy Yard in September 2013, and the leak of classified information by NSA contractor Edward Snowden, Sims focused much of his presentation on insider threats and how they can be mitigated. He emphasized the need to prevent further incidents and cited the important partnership between the U.S. government and industry in maintaining a strong industrial security program.

Keynote Speaker

Elana Broitman, Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy, was the keynote speaker on the first day. Broitman gave her perspectives on foreign investment in the defense industrial base and the current and future climate for the Department of Defense (DoD) in the globalized market and shared her experiences within DoD, industry, and on Capitol Hill.

Cloud Computing

Trevor Odell, Director of Information Security and Assurance for BAE Systems, Inc., presented "Security – A Cloud Future? Looking Backward to See Forward," to both audiences. The briefing focused on cloud computing types and drivers, as well as cloud connectivity and migration.

Odell also shared BAE's cloud use models and his perspective on key cloud challenges. He portrayed the challenges BAE faced in implementing its cloud network, which was beneficial for an audience dealing with similar challenges, and emphasized the fact that "the cloud is not coming, it's already here."

Discussion Panel

Experienced Outside Directors/Proxy Holders John Currier, Joanne Isham, and Jim Wolbarsht held a discussion panel and answered questions regarding the relationship between FSOs and their associated foreign parent companies. The panel discussion also focused on the additional roles and unique challenges a FSO encounters while under FOCI mitigation.

DSS subject matter experts from across the agency presented briefings on various topics during the conference, to include Affiliated Operations Plans, Facilities Location Plans, cyber security, the risk equation, supply chain risk management, and the annual DSS publication, "Targeting U.S. Technologies – A Trend Analysis of Cleared Industry Reporting."

A panel of DSS experts also fielded questions from the audience at the end of the second day. Discussion points included topics ranging from facility clearance processing timelines to questions regarding affiliate visit policies.

DSS has tentatively scheduled the next FOCI conference for early spring of 2015. For more information about the DSS FOCI program, visit the agency website at: www.dss.mil/isp/foci/foci_info.html.

IMAGES AT LEFT, FROM TOP: Trevor Odell, Director of IT Security and Assurance for BAE Systems, Inc., gives a presentation on corporate security and the cloud. | Outside Director Brett Lambert, former Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy, answers a question. | FOCI Operations Division Chief Ben Richardson delivers his presentation. | FOCI Program Manager Jarvis Waters answers questions from the audience. | Outside Director Jim Wolbarsht, Proxy Holder John Currier, and Proxy Holder Joanne Isham participated in a panel and explain the importance of Facility Security Officers working alongside Outside Directors and Proxy Holders.

A Q&A WITH **JIM KREN**, DSS DEPUTY DIRECTOR

Jim Kren was appointed as Deputy Director of DSS on Sept. 11, 2011. Kren began his career with the Defense Mapping Agency (DMA), later the National Imagery and Mapping Agency (NIMA). During his 13 years with DMA/NIMA, he held a variety of positions with increasing responsibility, to include systems engineer, physical scientist, cartographer and geographer. He then went on to serve six years in the Office of the Secretary of Defense.

Kren was first promoted to the senior level in 2004 while serving in the Office of the Under Secretary of Defense for Intelligence. Prior to his assignment to DSS, Kren served as the Director of Innovation and Collaboration, Intelligence Systems Support Office (ISSO), Office of the Secretary of the Air Force. During his tenure with ISSO, he was assigned to the North Atlantic Treaty Organization in Brussels, Belgium, first as special advisor to the Assistant Secretary General for Defense Investment and then as General Manager of the Battlefield Information Collection and Exploitation Systems Agency.

What is the role of the Deputy Director at DSS? How does your role support/complement that of the Director?

The deputy position has several roles at DSS to include identifying and addressing policy, resources and program level issues that affect our ability to execute the DSS mission. I am focused on internal DSS operations and work closely with the directors of Counterintelligence, Policy and Programs, Field Operations and the Center for Development of Security Excellence. I am also externally focused on strengthening relationships and partnerships with the Office of the Secretary of Defense and other senior stakeholders across the Department and the National Industrial Security Program. Additionally, I have key responsibility for the agency's overall governance process as well as DSS enterprise level decisions.

I support the Director by serving as a consultant or advisor. In many ways I am a sounding board for the Director when discussing the mission and operations of the agency. I have sought to be an active listener across DSS and tried to maintain peripheral vision on the internal challenges and the external environment affecting the position of DSS within the overall Defense Enterprise.

How are you effecting change at DSS to position/prepare the agency for the future?

For the last two and a half years, I have been focused on strengthening overall accountability and responsibility across our mission areas and enhancing our planning processes and acquisition strategies to improve consistency in our activities. In some ways, I have been assisting the Director in challenging the status quo. For instance, how can DSS execute our various mission sets in order to achieve better outcomes? We are continuing to look at our priorities and will work closely with the mission directorates to invest in the agency's future by identifying, engaging and enabling future leaders, developing methods to conduct risk mitigation and cultivating partnerships with cleared industry. We can also prepare for the future by advancing tighter integration in how DSS executes our mission. This may not necessarily be accomplished through an organizational structure though. It might mean a tighter operating relationship across the agency when pursuing our most important missions and ensuring compliance to deter our adversaries from stealing and exploiting what cleared industry possesses, develops and delivers to the U.S. government.

Your bio shows a broad range of professional experience. How does that diverse background help you in your current position?

I think my background provides a certain level of awareness and appreciation of the complexity involved with leading large organizations — as well as an appreciation of how the broad strategies, policies and missions of the defense enterprise are developed, planned and executed. The knowledge I have gained from these previous experiences has helped me to pinpoint DSS' contribution to the overall DoD mission.

Additionally, I think my professional experiences have enabled me to develop a set of "models" for dealing with uncertainty, challenges and opportunities. Having witnessed similar challenges and risks before, I can rely on an established framework to lead and leverage opportunities as they develop.

You have emphasized the need for a comprehensive governance structure for DSS. Why do you think that's important and what progress has been made?

Governance, in general, is a structure for dealing with issues, challenges and the need to make informed decisions. Our comprehensive governance structure is intended to improve and enhance broader communications across DSS and awareness within the decision making process. I am hopeful that this progress will garner a greater acceptance of change, will build consensus and develop good courses of action for all types of decisions we need to make as a defense agency.

Since 2013, we have been committed to improving the Executive Steering Committee (ESC). I believe we have improved our structure and the operations tempo of this activity and we have increased participation at all levels across DSS. The Enterprise Planning and Integration Council consists of leaders and action officers (GG-15 level) from across DSS. They review and discuss initiatives and topics that affect the DSS enterprise, and prepare recommended agenda items for the Deputies' Council (DC). The DC (DISL/deputy level) makes decisions or offers input before topics and initiatives reach the ESC. We also adjusted the structure of the ESC meeting itself to ensure discussion of key challenges and issues in an open and forthcoming way as seniors. While we have made progress, we still have more to do. We are currently developing our DSS Strategic Plan 2020 and leveraging all levels of our ESC governance structure.

You've also been very focused on automation initiatives at DSS. Why are these important and how will they position DSS for the future?

One of the reasons I was so interested in the opportunity to serve at DSS was to help shape future information technology developments, enhancements and the way DSS delivers those IT services to our internal workforce and to our external stakeholders and partners. When prioritizing the fiscal year 2015 Program Objective Memorandum (POM), basically our budget, the Director and I quickly realized our two top priorities for the next POM FY15-FY19. The first priority is to retain our unique and small workforce by protecting the size of our current workforce. The DSS' mission is manpower intensive and requires real presence and personal contact with our stakeholders.

The second priority is to optimize that skilled workforce with technology. That's why both the National Industrial Security System (NISS) and the NISP Contract Classification Specification (NCCS) are key investments over this POM cycle. These types of information technology solutions are imperative to maximizing the time our field personnel have available to work directly with our stakeholders and partners across the NISP. We need to deliver new capabilities to achieve tighter integration and achieve a data driven environment across the NISP. This force multiplier will enable the agency to remain viable and relevant well into the future. The Department and the Office of the Director of National Intelligence are supportive of DSS's investment and development efforts in these IT enhancements; however, we must continually present the rationale and cost effectiveness of our approach.

I am very impressed and encouraged by the continuing work on the NISS requirements gathering process by the field and headquarters personnel, many who have been personally involved in capturing the current state assessment and developing our key mission areas. They are doing a fantastic job of defining the system for our future and I urge everyone to check out the comprehensive and up to date NISS SharePoint site. As a defense agency, we have reached almost every office at the Office of the Secretary of Defense level to ensure support and advocacy for these efforts. As we proceed further, we will directly involve cleared industry in future phases of this effort.

Another key IT service initiative is the development of the NISP Contract Classification System or NCCS. There is a critical shortfall in the ability of DoD and other federal agencies to manage information related to the security requirements for classified contracts. Since 2012, DSS has been developing awareness and requirements to address this shortfall. The NCCS effort is very important because it directly responds to a recent DoD Inspector General recommendation that DoD develop a central repository for this type of contract information.

Another initiative you championed was the Office of Innovation. What is its purpose and how is it changing how DSS operates?

The driving purpose behind developing a formalized innovation effort at DSS has been to capture ideas, at all levels, and turn them into viable solutions that strengthen the way we conduct our mission and the manner in which we support our men and women executing the mission. The main efforts of the Office of Innovation are to establish a framework by which DSS can move from the 'ideation' stage to an implementation stage that includes analytic rigor and investment options. The DSS innovation efforts have been focused on both materiel and non-materiel solutions to improve and support our field operations. From my perspective, innovation is critical to facilitating ideas and strengthening our overall integration. I expect the office will concretely enhance our ability to quickly explore ideas and solutions while providing "an inject" into our Governance structure and resource investment decisions. >>

As you look outward and to the future, what do you see as the major challenges and opportunities for DSS in the next year, five years?

The major challenge I see over the next year to two years will be our ability to be properly position DSS for approaching changes that the DoD and other external drivers may require of us as a defense agency. This means we need to ensure that we are properly positioned to adapt and adjust and remain relevant and recognized as a key contributor to the defense enterprise.

Some of the potential challenges and opportunity areas include insider threats internally, within the Department and across the NISP; increased focus on the protection of valuable technical and controlled data within industry; potential increased responsibility for DSS to oversee Committee on Foreign Investment in the United States mitigation; and an expectation that DSS delivers on NISS and related IT enhancements.

In order to be properly positioned for approaching changes we must make good resource decisions and that will remain a major challenge over the next two years. As a defense agency we must continue to make sound investments in our people and capabilities that will have the highest payoff for our enduring mission of managing risk within cleared industry.

I see two main opportunities over the next two years. The first is to continue telling the DSS story by enrolling advocates for DSS and ensuring our value is clearly understood across all of our stakeholder and partners. This will require DSS to continue to listen and bring in reciprocal value by enabling our partners' missions and defense enterprise activities.

The second opportunity may be an outcome of the Defense Strategic Guidance from the 2014 Quadrennial Defense Review (QDR). The QDR rebalances and reduces the overall size of the Joint Force; however, investment decisions will ensure the U.S. maintains a technological edge over potential adversaries. This will call for DSS's involvement and expertise to safeguard the nation's investments in technological advances and making certain they are not compromised or diminished as the Department looks to deploy these advanced capabilities.

TRIAGE OUTREACH PROGRAM ENHANCES COMMUNICATION, STRENGTHENS PARTNERSHIP WITH INDUSTRY

By Ryan Dennis
Industrial Security Field Operations

Partnership is important! The key to building and maintaining an effective partnership is communication and understanding.

Last year, the Triage Outreach Program (TOP) was established to enhance communication and assess risk at facilities not slated for assessments during the current year. This new program not only improves communication between DSS and industry but helps companies identify vulnerabilities and stay up-to-date on changes in the security environment.

How does TOP work? Facilities are selected each quarter using a risk-based approach. Once selected, the Facility Security Officer (FSO) will receive an email from DSS detailing each step in the program. The FSO will then receive a phone call from a DSS representative and will be asked a series of questions pertaining to their security program.

The questions focus primarily on reporting requirements (i.e. suspicious contacts, adverse information, changed conditions, etc.), but the call is a guided discussion about the security program at the facility. This is a great opportunity to ask questions! At the conclusion of the call, DSS will work with the FSO to address any issues or mitigate identified vulnerabilities.

To date, TOP has reached more than 1,200 facilities nationwide. Approximately 54 percent of the outreach contacts have resulted in identification of one or more vulnerabilities. In each case, DSS was able to help the FSO mitigate vulnerabilities and reduce the risk to classified information. Industry feedback on the program has been positive, and Field Operations is looking to expand it to reach more facilities each year. As the program expands and changes, DSS will continue to provide updates and training to ensure full transparency.

iGUARDIAN IMPROVES CLEARED CONTRACTOR REPORTING

By Anthony T. Colliluori
Federal Bureau of Investigation Liaison to DSS

Suspicious contact reports from industry are vital to identifying indications of intelligence threats. Yet the reporting process can hinder timely reporting, as the need to flesh out the report takes time and effort.

Conversely, feedback on the consequence and value of the reporting is important for industry to see tangible results but is an absent part of the process. A new system, projected for release in 2015, will resolve many of these issues, while also satisfying most federal cyber incident reporting requirements.

The iGuardian will be implemented incrementally as a means of resolving issues during the development phase and will build on the current Federal Bureau of Investigation's (FBI) terrorism reporting system, called Guardian. Developed by the FBI, iGuardian will resolve many identified reporting challenges while simultaneously providing a much desired feedback function to encourage greater public-private partnership.

By incorporating lessons learned, operational requirements and industry input, iGuardian is a significant development in information sharing, threat and incident reporting management, and industry-government partnership. This modified Guardian system is prefaced with an 'i' for industry and feeds the larger Guardian system operating across the unclassified and classified domains.

The iGuardian website will feature four reporting options: cyber; counterintelligence; terrorism; and criminal. Each option presents unique submission forms addressing specific issues and questions pertinent to the selected topic area, and will support submissions that deal with more than one of the four areas.

Just as iGuardian streamlines the reporting of cyber, counterintelligence, terrorism and criminal activity, it also simultaneously sends notifications to multiple government agencies. For cleared industry, a submission triggers notification to the FBI and DSS to satisfy reporting obligations specified in the National Industrial Security Program Operating Manual (NISPOM). As the program expands, additional recipients will be added to the form as a part of the notification process.

Another feature is the option to include malware with submissions, which will be sent to the FBI and the Defense Cyber Crime Center for analysis. A report history and action summary is visible to cleared contractors based on its Commercial and Government Entity (CAGE) code.

The reporting process will also allow the submitter to attach notes to a particular report. These notes can detail what intelligence has been gathered about the threat or incident, and it will have a protected platform for law enforcement/counterintelligence agents to share unclassified findings with each other and with the contractor in a more substantive way.

iGuardian will have a substantial impact on cleared contractors, as it will help those who may not have in-depth cybersecurity programs to better understand the events and outcomes of their reporting. Contractors of all sizes will benefit from the reduced reporting burden answered by a single reporting point with simple forms and greater feedback.

From the government's perspective, the near instantaneous sharing of information between DSS and the FBI at the time of the contractor's submission will contribute significantly to rapid analysis and countering of the threat. It will help prioritize the significance of each report and assist in identifying information gaps.

With knowledge of the gaps, the DSS counterintelligence agents can more effectively inform the contractor on the threat and its effect, and partner to characterize the threat and possible countermeasures, raise alertness to the continuing threat, and fine tune the reporting and response processes.

PERSONNEL SECURITY MANAGEMENT OFFICE FOR INDUSTRY INITIATIVES

By Zaakia Bailey
Personnel Security Management Office for Industry

NCMS Board of Directors Tour PSMO-I

On Jan. 14, 2014, members of the NCMS Board of Directors visited the Personnel Security Management Office for Industry (PSMO-I) for an onsite meeting. Attendees included President, Leonard Moss; Vice President, Debbie Young; Secretary, Dennis Arriaga; Seminar Program Chair, Tameka Watts, and Directors, Aprille Abbot; John Dean; Quinton Wilkes; Kat Boyer; Sheryl Daniels; and Catherine Kaohi.

The purpose of the meeting was to allow the board the opportunity to tour the new Hanover facility and learn about current trends and future policy affecting security specialists. At the same time, the NCMS representatives shared their insights and provided feedback to the agency. Topics of discussion included the current status of personnel security investigation submissions, electronic fingerprint submissions, JPAS Data Quality Initiatives, JPAS account management, and a future industry portal in the Case Adjudication Tracking System (CATS).

PSI Submissions

There are currently under 3,000 Electronic Questionnaires for Investigations Processing (e-QIP) forms in the queue for review and submission to Office of Personnel Management (OPM); down from a high of 13,992 in November 2013. That backlog was a result of the October 2013 government shutdown and a delay in the Fiscal Year 2014 funding authorization. PSMO-I will continue to work through the backlog and return to a steady state of 1,200 pending submission. For facilities that submitted an e-QIP for a subject who no longer requires a clearance, PSMO-I requests that JPAS be updated with a separation date so the e-QIP may be stopped.

Electronic Fingerprints (eFP)

In a memorandum dated July 29, 2010, the Under Secretary of Defense for Intelligence (USD(I)) issued a requirement for Department of Defense (DoD) components to transition to electronic capture and submission of fingerprint images in support of all background investigations by Dec. 31, 2013.

As of February 2014, 87 percent of industry fingerprint submissions were electronic. If a company needs additional information regarding electronic fingerprint submission, the eFP Implementation Guide can be found at www.dss.mil/documents/psmo-i/eFP_Guide_Feb_2014.pdf. The guide provides several options, and companies can determine which work best for them.

Interim Clearance Process Change

Under Secretary of Defense for Intelligence, Michael Vickers recently signed the DoD policy that will soon change the process for industry interim clearances. The new policy, once effective, mandates the minimum requirements for an interim Secret or Confidential eligibility as:

1. **Investigation scheduled**
2. **Favorable review fingerprint results**
3. **Favorable review national databases**
4. **Favorable review of the SF-86**

DSS is currently working with OPM to automate the electronic delivery of the Advanced National Agency Check (NAC) to support the e-Interim Process. DSS will coordinate implementation with USD(I) and will advertise the implementation date to industry at least 30 days in advance.

Data Quality Initiative (DQI) 68982

The Defense Manpower Data Center (DMDC) JPAS team, in coordination with DSS, began running Data Quality Initiative (DQI) 68982 in January 2014, separating over 300,000 industry person categories with no owning or servicing Security Management Office Code relationship in JPAS. The second run was in March 2014 and separated over 30,000 more person categories.

This DQI will run monthly, targeting all industry categories without a valid Owning/Servicing relationship. However, the DQI will not impact records identified as Key Management Personnel (KMP).

JPAS Account Management

In addition to DMDC's ongoing DQI efforts, U.S. Cyber Command recently issued Task Order 13-0641 that decreased its inactive account deletion deadline from 90 days to 45. Consequently, the JPAS team will soon begin deactivating accounts that meet the criteria.

Facility Security Officers (FSOs) that have their account terminated due to inactivity will have to reinitiate the process of obtaining a new JPAS account. This change will not affect the current 30-day account lock due to inactivity. To avoid any loss of access, FSOs should log on to JPAS at least weekly.

Future CATS Portal

One of the main objectives of the PSMO-I is to be industry's liaison to the DoD Consolidated Adjudication Facility (CAF). In order to increase support to industry, PSMO-I has been providing guidance on National Industrial Security Program (NISP) requirements in support of CATS Version 4 that is set for testing in the fourth quarter of FY14 and will deploy soon after.

One of the enhancements will be a KMP Program Designator code to aid in expediting the processing of KMP adjudications and reporting. Another enhancement will be an industry portal that will enable FSOs to receive information from PSMO-I and the DoD CAF, and will allow sharing of documents with a "browse and attach" function. For example, through the portal, FSOs will be able to upload the SF312, "Non-Disclosure Agreements," and other required documentation.

Stay in Touch

The PSMO-I continues to partner with industry to enhance the NISP personnel security program. PSMO-I hosts a monthly teleconference with members from Industry, DMDC, OPM, USD(I), and DSS to discuss and resolve personnel security issues. PSMO-I also hosts bimonthly webinars on topics recommended by industry.

For more information, see the PSMO-I website at www.dss.mil/psmo-i/index.html

ODAA UPDATES TOOLS FOR

CERTIFICATION AND ACCREDITATION

The Office of the Designated Approving Authority (ODAA) recently unveiled an updated set of system security plan (SSP) templates and accompanying Process Guide designed to assist industry Information System Security Managers (ISSMs) in completing system accreditation tasks.

The updated ODAA Process Guide was released in November 2013, with a required implementation date of May 15, 2014. The Process Guide is used as a desk reference and "how to" guide during completion of the complex tasks associated with obtaining DSS accreditations for information systems.

The process guide provides numerous "step-by-step" instruction sets and consolidates a variety of procedural requirements into an "easy-to-use" reference document. Although some industry ISSMs may refer to the Process Guide only on occasion, it is an invaluable resource for new ISSMs who use it not only as a guide, but also as a training aid.

The updated ODAA SSP templates serve as a simplified structure for ISSMs to follow when documenting security configurations and special procedures applicable to information systems. The SSPs are reviewed by DSS Information Systems Security Professionals (ISSPs) and upon completion of a successful onsite verification of a system's configuration, the system attains accreditation.

The accreditation is issued by the DSS Regional Designated Approving Authority (RDAA) and serves as official approval from the U.S. Government for the system to process classified information.

The Process Guide, when used in conjunction with the SSP templates, directs the ISSM through the requirements for obtaining accreditation for information systems ranging from a simple desktop computer to a complex wide area network spanning the country.

The resulting documentation is the government's official record of a system's configuration and the procedural requirements the user of the system is required to follow. The SSPs are maintained as official records by DSS ODAA.

Both the ODAA Process Guide and SSP templates represent a significant collaborative effort between DSS and industry partners. While drafting each of the documents, DSS staff met with industry representatives to discuss the content and format. Although DSS specified the requirements, industry had 30 days to review and comment on the documents. As a result of the collaboration, the final coordination process was significantly improved and resulted in better products.

The Process Guide and templates have evolved over a number of years into an effective approach to providing concise guidance and consistent documentation for industry. By properly using the tools provided, ISSMs, ISSPs, and the ODAA program have been able to develop an efficient process that results in properly secured information systems while providing for impressive timeliness and turnaround times for accreditations.

Benefits of the Updated ODAA Manual and SSP Templates:

Saves Time — The templates provide instructions and information to guide the ISSM through the completion process so there is no need to search for guidance or instructions for completing the security plan. The template "prompts" the ISSM to complete the blocks of information required for system accreditation. Using the templates minimizes confusion and rework, thus saving time and resulting in a compliant document.

Consistent Format for Reviewers — Using a consistent format for security plan documentation improves the review process. ISSPs reviewing the document are familiar with the "flow" of the required information and can easily identify specific blocks of information during the review process.

User-friendly PDF Format — As the name implies, PDF templates are portable across operating systems and can be completed and reviewed on a variety of platforms. The updated templates dynamically adjust to enable specific fields for information required depending upon the type of system being documented, such as local area networks, wide area networks, or standalone computers.

WHAT IS SLTPS?

By Booker T. Bland
Industrial Policy and Programs

The need to share timely, relevant, and actionable intelligence among federal, state, local, and private sector partners to enhance national security is undeniable. Sharing the information in a safe and secure environment is equally as important.

To safeguard and govern access to classified national security information shared by the Federal Government with State, Local, Tribal, and Private Sector (SLTPS) entities, President Obama signed Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector (SLTPS) entities," on Aug. 18, 2010.

The purpose of Executive Order 13549 was to ensure that security standards governing access to, and safeguarding of, classified material are applied in accordance with existing Executive Orders (EO) such as:

- **EO 13526** of Dec. 29, 2009 *("Classified National Security Information")*
- **EO 12968** of Aug. 2, 1995, as amended *("Access to Classified Information")*
- **EO 13467** of June 30, 2008 *("Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information")*
- **EO 12829** of Jan. 6, 1993, as amended *("National Industrial Security Program")*

Simply put, EO 13549 put in place a governance and oversight structure to establish processes, procedures, and to promote the uniform application of security standards for providing access to, and safeguarding of, classified information when shared with the SLTPS entities. Under the EO, the National Security Advisor provides overall policy guidance for the SLTPS program. The Secretary of Homeland Security is designated as the Executive Agent for the program, responsible for implementing and overseeing its administration in consultation with the affected executive departments and agencies. It also requires the concurrence of the Secretary of Defense, the Attorney General, the Director of National Intelligence (DNI), and the Director of the Information Security Oversight Office (ISOO).

EO 13549 does not apply to private sector personnel who are employed by a company or other commercial entity that falls under the National Industrial Security Program Operating Manual (NISPOM) and EO 12829. It also does not apply to private sector entities where classified information is, or will be physically stored. Under EO 12829, the cognizant security agency provides program management, oversight, inspection, accreditation and monitoring of all private sector facilities that physically store classified information.

SLTPS Policy Advisory Committee (SLTPS-PAC)

The SLTPS-PAC was established to advise the President, the Secretary of Homeland Security, the Director of ISOO, and other executive branch officials on all matters concerning the oversight of the SLTPS Program. The SLTPS-PAC is responsible for discussing program-related policy issues in dispute to facilitate their resolution and to recommend changes to policies and procedures that are designed to remove undue impediments to the sharing of information under the SLTPS program.

Current government members of the PAC include the ISOO Director, who serves as the Chair; designees from the departments of Homeland Security, State, Defense, Justice, Transportation, and Energy, the Nuclear Regulatory Commission, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Federal Bureau of Investigation. Members may also include employees of other agencies and representatives of SLTPS entities, as nominated by any committee member and approved by the Chair.

Further information concerning the SLTPS-PAC's charter and bylaws, meetings, and minutes, and contact information for its members is available on the ISOO website at http://www.archives.gov/isoo/oversight-groups/sltps-pac/

Copies of the Executive Order 13549 in its entirety can be found at www.archives.gov/isoo/policy-documents/eo-13549.pdf.

What is a Tribe? As defined in EO 13549, "Tribe" means any Indian or Alaska Native tribe, band, nation, pueblo, village, or community that the Secretary of the Interior acknowledges to exist as an Indian tribe as defined in the Federally Recognized Tribe List Act of 1994 (25 U.S.C. 479a(2)).

CDSE COMPLETES SELF-STUDY FOR ACCREDITATION REAFFIRMATION

By Julie Wehrle
Center for Development of Security Excellence

The Center for Development of Security Excellence (CDSE) completed its self-study report as a part of the accreditation reaffirmation by the Commission of the Council on Occupational Education (COE) in March 2014. CDSE was first accredited by COE as the Defense Security Service Academy (DSSA) in 2002.

CDSE's accreditation is subject to reaffirmation every six years, with the most recent reaffirmation in 2008. The self-study is a standard requirement of both the accreditation and reaffirmation processes. COE accreditation status is granted to an educational institution or program that meets or exceeds stated criteria of educational quality and student achievement.

Why CDSE Accreditation is Important

Accreditation is required by DoD policy, which mandates accreditation by an entity recognized by the U.S. Department of Education. DoD Instruction 1400.25, Volume 410, DoD Civilian Personnel Management System: Training, Education, and Professional Development (TE&PD) requires implementation of TE&PD activities and programs for DoD civilians at the highest possible level of academic quality and cost-effectiveness, consistent with standards established by external accreditation and certification entities recognized by the U.S. Department of Education when applicable standards exist.

Having and maintaining COE accreditation status is important for CDSE's students, stakeholders, and members of the DoD security, intelligence and industrial security communities. The accreditation status validates that CDSE meets COE standards for institutional operation and educational excellence. It also signifies that CDSE's services are sound and that CDSE meets its responsibilities to those who benefit from or avail of their services and products.

COE accreditation processes consider the characteristics of the whole institution including educational offerings, student personnel services, financial status, administrative structure, facilities, and equipment. To maintain COE accreditation status, institutions must file annual reports, report changes, and maintain documents related to COE workshop attendance, accreditation activities, and advisory committee meetings. The self-study is required for initial COE accreditation and for each reaffirmation.

The CDSE Self-Study

The self-study provides a venue for examining qualifications for accreditation reaffirmation and serves as an evaluation and planning vehicle for improvement of services. The self-study requires CDSE to review, evaluate, and re-evaluate what they do, why and how they do it, determine if they are in compliance with COE accreditation requirements, and discover improvements to programs and services. It also demonstrates to the CDSE community of students, stakeholders, and customers that there is a continuing evaluation, both internal and external, of CDSE services, products, processes, and procedures.

The COE self-study manual provides a detailed guide for conducting the self-evaluation which includes suggested methods for assigning staff and work, timetables, resources, and specific format requirements for the self-study report. As part of the accreditation reaffirmation process, a COE survey team of professional colleagues conducted an extended visit at CDSE to validate the CDSE self-study by reviewing CDSE's operation, educational programs, and documents on file.

Conditions, Standards, Objectives, and Criteria

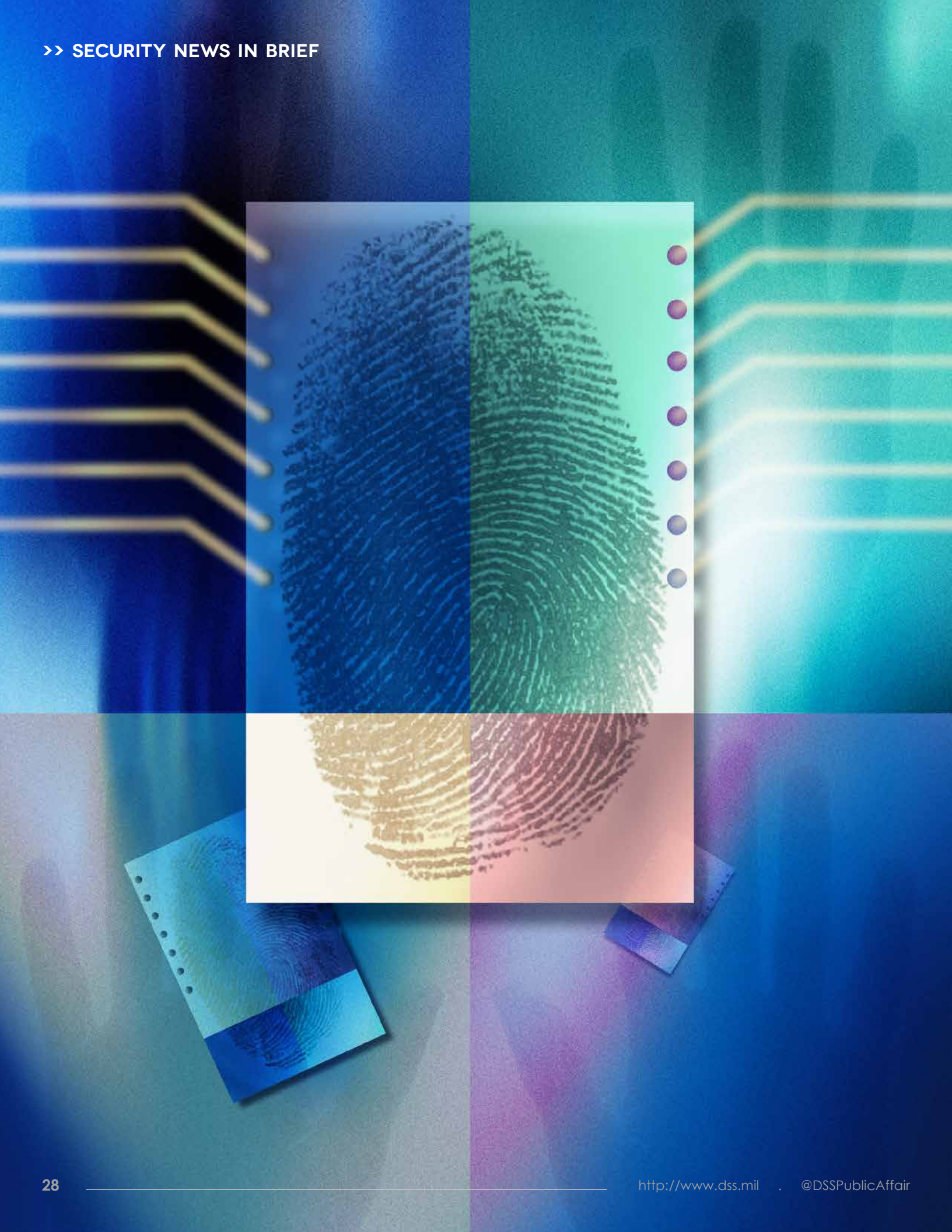
The self-study centers on accreditation conditions, standards, objectives, and criteria that apply to CDSE, and in turn, CDSE responds to each item with a narrative response and supporting documentation. There are 11 standards in the self-study, each with a different number of criteria that must be addressed.

CDSE Self-Study Report

The 2014 CDSE self-study was conducted over six months. A core group of CDSE staff members were selected as leads for the self-study standards, but this was not a simple checklist activity. The standards criteria provided in the self-study manual were guides used to discover what CDSE does, how they do it, and what documentation or evidence exists to prove it. Each standard and associated criteria were addressed in narrative format, with introductions, responses, challenges and solutions, and summaries. Most of the criteria responses required supporting documentation as evidence.

Garry Carter Jr., of the COE survey team, told the CDSE staff during a preliminary self-study visit that CDSE has "vision, constantly looking ahead. You know where you've been, where you've brought it to, and where you want to be." Kevin Jones, Director of the CDSE, said of the CDSE self-study and COE team review that CDSE is a "learning organization that looks forward to being better every year" and that "we are improved by external evaluation."

CDSE is committed to providing excellence in its education, training, products and services to the DoD security community. The COE self-study and accreditation affirmation demonstrate that commitment.



Industrial Security Oversight Certification Now Live in Production

In December 2013, the Department of Defense Security Training Council (DSTC) approved the cut score and business rules for one of the newest DoD specialty security certifications, the Industrial Security Oversight Certification (ISOC).

The ISOC is the second specialty certification under the Security Professional Education Development (SPēD) program and assesses candidates' knowledge on such competencies as: information security, classification management, incident response, information assurance/ cybersecurity, personnel security, physical security, industrial security, general security and the National Industrial Security Program (NISP).

It also addresses foundational concepts in facility security and clearance, general safeguarding requirements, facility surveys, and inspections. It is ideal for DoD and other U.S. government personnel (civilian and military) and contractors under the NISP who will be, or are already performing industrial security oversight functions either full-time or as an additional duty on behalf of a component or agency.

DoD and other U.S. government personnel (civilian, military, and contractors) who have been conferred the Security Fundamental Professional Certification (SFPC) are welcome to participate. For more information on the ISOC and other SPēD certifications, visit www.cdse.edu/certification/sped_what.html.

CDSE Releases New ISSP Training Program

The Center for Development of Security Excellence (CDSE) is pleased to announce the release of the National Industrial Security Program (NISP) Information Assurance (IA) Fundamentals (CS101.01) Course.

The NISP-IA Fundamentals Course employs an instructor facilitated eLearning environment that provides an in-depth program to standardize Information System Security Professionals (ISSP) training agency-wide. The course provides new ISSP personnel with a strong base to begin their DSS careers and allows experienced ISSPs the opportunity to earn credit for previously completed training.

"The new ISSP training curriculum is the first formal training program for DSS ISSPs," said Randy Riley, Assistant Deputy Director, Office of the Designated Approving Authority, "and represents a big step toward building a consistent baseline of knowledge across the ISSP workforce."

The course introduces the roles and responsibilities of the ISSP position via required readings, pre-recorded lectures and presentations, written assignments, quizzes, and a final exam. Students are also introduced to the ISSP apprenticeship and mentoring program that prepares ISSPs to perform their standard duties.

The intent for the ISSP training program is to ensure all ISSPs have similar competency and baseline knowledge. This ensures consistency throughout DSS' 45 field offices in support of the NISP in Information Assurance, including Certification and Accreditation requirements.

Security Asset Protection Professional Certification Achieves National Accreditation

On Jan. 15, 2014, the Security Asset Protection Professional Certification (SAPPC) was the second of three certifications under the SPēD Certification Program to receive national-level accreditation by the National Commission for Certifying Agencies (NCCA).

This follows the national accreditation of the first core security certification in December 2012, the Security Fundamentals Professional Certification (SFPC), which recognizes the significance of the SFPC and the rigor of its execution.

Accreditation by NCCA places the SAPPC certification on par with other professions in the financial, legal, and healthcare professions, such as the American Association of Critical-Care Nurses and the National Association of Social Workers.

DoD Manual 3305.13-M, "DoD Security Accreditation and Certification," mandates the Director of DSS to apply all certifications developed under the SPēD Certification Program to the NCCA (the nationally recognized certification accreditation body) through the Institute for Credentialing Excellence (ICE) for external accreditation.

DSS began the SAPPC accreditation process in February 2013 to obtain NCCA review. As part of the process, DSS engaged in an extensive application and standards review process using the DoD Security Training Council as its governing board.

The application package included statements and evidence to support compliance with NCCA's comprehensive 21 standards. It also covered all aspects of the SAPPC program including administration, assessment development, and recertification.

For more information on the SAPPC and other SPēD certifications, please visit www.cdse.edu/certification/sped_what.html.

THE HIGHEST BIDDER

Since April 2012, the DSS Operations Analysis Group (OAG) has received nine cases involving the discovery of export-controlled equipment for sale, without restrictions, on public, online auction websites.

Eight cases were reported to DSS by a cleared contractor, and the ninth case was reported by another government agency requesting information and assistance.

This article is designed to provide case highlights, best practices and information about government resources available to cleared contractors working with and producing export-controlled products and technology.

Chronology of Cases

April 2012

A cleared contractor discovered an export-controlled laptop for sale on an online auction website. The company reported the discovery to DSS, who then reviewed the case and referred the matter to multiple government agencies.

A second case during the same month involving a different company concerned a cleared individual suspected of diverting U.S. military property for personal gain. The individual was also under investigation for illegally exporting U.S. military equipment without a State Department license.

DSS was notified of this matter by another government agency conducting an investigation, who requested information and assistance.

February 2013

A cleared contractor reported several of its products for sale on an online auction website. The company's Director of Business Development discovered the product availability during a routine search of online auction websites. After the company reported the matter to DSS, the case was reviewed and referred to several government agencies.

March 2013

A cleared contractor reported one of its sensitive, export-controlled, hand-held encrypted radios offered for sale by a foreign entity on an online auction website. The auctioned item was noticed by the company, which immediately reported it to DSS. After case review, the matter was referred to several government agencies.

April 2013

A cleared contractor advised DSS that one of its sensitive export-controlled items, which had been previously sold to another cleared contractor, was for sale on an online auction website. The cleared contractor purchased back the item through the auction website. After review of the case and the circumstances involved, DSS referred the matter to five government agencies.

Later in the month, in a separate matter, a second contractor discovered its export-controlled products being sold online by another vendor. The facility security officer of the company confirmed that the products were export controlled under International Traffic in Arm Regulations (ITAR) and that seven products in total were listed for sale. Each product was sold, and DSS was notified. After case review, the matter was referred to six government agencies.

May 2013

A cleared contractor found "For Official Use Only" blueprints and diagrams for sale online. The items were related to work projects the contractor performed for its government contracting activity (GCA). After the case was referred to DSS and reviewed by the OAG, the information was shared with a working group involving two other government agencies.

In addition to these cases, two additional cases (June and July 2013, respectively) involved a cleared contractor discovering export-controlled information being sold online. In the first discovery, the case was referred to two government agencies. In the second, DSS referred the matter to three government agencies.

Best Practices

The sale of export-controlled equipment and technology on public, online auction websites, without regard to export-control requirements, places U.S. technologies and

capabilities at risk. In addition to the illegality of selling export-controlled products without a license, the identity and motive of an online buyer often cannot be determined.

The OAG has found that some cleared contractors actively monitor online auction sites for the sale of export-controlled products they produce. This has been identified as a best practice for early detection of the sale of controlled equipment and technology.

What We Do

When the OAG receives a case involving the sale of export-controlled technology on an online auction website, they conduct a comprehensive and thorough review of the case and technology involved. After determining the GCA and agencies with a vested interest, technology, and any other factors that may be present, the OAG refers the matter to those agencies with enforcement and investigative authority.

Regulations, Laws & Additional Information

According to the U.S. Department of State, "The U.S. government views the sale, export, and re-transfer of defense articles and defense services as an integral part of safeguarding U.S. national security and furthering U.S. foreign policy objectives.

The [U.S. Department of State]Directorate of Defense Trade Controls (DDTC), in accordance with 22 U.S.C. 2778-2780 of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulation (ITAR) (22 CFR Parts 120-130), is charged with controlling the export and temporary import of defense articles and defense services covered by the United States Munitions List."

(See the DDTC web site at www.pmddtc.state.gov/index.html).

The Export Administration Regulations (15 CFR 730-774) control dual-use technologies and are administered by the Department of Commerce, Bureau of Industry and Security .

(See the Bureau web site at www.bis.doc.gov).

Recommended Training

The DSS Center for Development of Security Excellence (CDSE) provides information security shorts on topics associated with the protection of classified information. CDSE also provides eLearning courses in International and Physical Security.

(Access the security shorts at www.cdse.edu/catalog/index.html)

PROTECTING THE PERSON

State-of-the-Art Body Armor through the Centuries

To mitigate the advantage that our latest technological developments confer, our adversaries target information and technology in cleared industry. DSS, in concert with cleared industry, works to protect technology to prevent or delay the adversaries' ability to counter our latest weapons. This prolongs the advantage of the latest technologies and provides greater return on the investment in these high-tech systems.

Evolution of military technologies transforms the battlefield. Offensive and defensive technologies evolve hand in hand. New weapons systems lead to the need to develop more potent weapons, countermeasures, or protective systems. An example of this transformation of the battlefield through symbiotic evolution is body armor.

Stone Age warriors used layered leather shirts and/or carried hide shields to protect themselves against flint-tipped arrows. Advancements in technological capabilities led to further evolution in both arms and armor.

Revolutionizing Warfare

Metalworking revolutionized warfare. With the development of stronger bronze armor, stone axes and clubs could batter an opponent but were unable to do serious damage.

In the 7th century BCE, Greek Hoplites wore bronze helmets, breast plates, and shin guards and, perhaps most famously, carried bronze-plated shields, all of which protected against swords and spears of the same material. The Hoplites' most effective protection was the shield: the unit would form into a compact group surrounded by a shield wall that was nearly impenetrable.

Further advances in metallurgy introduced iron and eventually steel. The most dominant form of armor during the Iron Age was chain mail. It was designed to defend against stabbing and slashing weapons, and variations remained in use from the 1st through the 17th centuries. But mail was useless against blunt-force hits from weapons such as the hammer or the broad-bladed swords of the era that could render crushing blows.

Soldiers began supplementing their chain mail with small plates of steel to better protect the chest and head. In response, plate armor gave rise to the mace, a club-like weapon that could break bones even when shielded by armor. Later versions of the mace incorporated spikes capable of piercing armor.

Wearing A Full Suit

The refinement of the longbow and the advent of the crossbow made the mail covering knights' extremities ineffective. The next step was a full suit of plate armor.

By the end of the 15th century, this form of body armor was standard issue for knights. They still wore chain mail as well, but under the plate armor, to provide additional protection at the joints. The full suit of armor was virtually impenetrable to the longbow, axe, and broad-bladed sword.

However, despite the inclusion of chain mail, joints remained the most vulnerable areas. The first weapon to exploit this weakness was the modified sword, which evolved toward a narrower blade, better able to penetrate mail. Later, the war hammer, halberd, and poleax also incorporated elements capable of piercing armor. But the most effective counter-armor weapon remained the crossbow — until the invention of firearms.

Against early firearms, a suit of armor could still protect its wearer. But as firearm technology progressed, armor became less effective. For armor to be firearm-resistant, it had to be so much thicker it was impractical due to sheer weight. Over the next four centuries, soldiers increasingly abandoned body armor in favor of mobility on the battlefield.

Yet the break was never complete. Foot soldiers continued to use back and breast plates throughout the 18th century. There is even evidence that some soldiers used plate armor during the American Civil War. However, these plates were not military-issue and were not effective against all firearms.

Stopping Bullets

In the late 19th century, Japan and Korea simultaneously developed the first version of the modern bulletproof vest. They discovered that layered silk fabric could stop black powder-propelled bullets. In the early 20th century, an American priest and a Polish inventor devised a vest that wove a steel plate between layers of silk. This vest protected against lower-caliber bullets.

Helmets, which had been largely abandoned in the late 16th century, resurfaced in World War 1. At the start of the conflict, despite the dramatic advancements in weaponry, countries deployed their troops with almost no body armor. The trench-style warfare essentially protected soldiers' lower bodies, but their heads were left exposed. Militaries quickly developed and deployed the first modern steel helmets to protect against bullets and shrapnel.

By World War 2, the military began issuing "flak" jackets to bomber crews to help protect them from anti-air artillery rounds. The 22-lb. vest consisted of steel plates sewn into a nylon vest, and was designed specifically to protect the wearer from shrapnel. But these vests were ineffective against handguns and still too heavy for general combat use.

In the 1950s, the vests were upgraded by substituting lightweight fiber-laminate plates for steel. However, they were still primarily designed to protect the wearer from shrapnel, providing little protection against rifle rounds.

Still Used Today

Kevlar, developed in the late 1960s, fundamentally changed personal body armor protection, and is still used today. It protects against small-caliber rounds and grenade fragments; ceramic inserts in the armor offer even greater protection from shrapnel and rifle rounds.

Every advance in military technology creates an imperative for a corresponding defense mechanism and/or counterweapon. Foreign entities target a wide array of technology resident in cleared industry. Any compromise of information about our military gear can reduce its impact on the battlefield and imperil our warfighters.

In February 2014, the DSS Freedom of Information Act (FOIA) office received a call from the Defense Manpower Data Center (DMDC) regarding some recently discovered boxes containing case files from the 1970's. According to DMDC, the files pertained to criminal investigations performed by the Defense Investigative Service (DIS) — the forerunner to DSS.

About the Defense Investigative Service

In a November 5, 1971, memorandum, President Richard Nixon directed the establishment of a single office of Defense Investigation. Following internal debates about the exact missions of the new agency, the Secretary of Defense, Melvin R. Laird, approved the time-phased creation of a Defense Investigative Service (DIS).

The agency commenced operations on April 1, 1972, and on October 1, 1972, all Personnel Security Investigation (PSI) field investigative resources and investigators were transferred from the Military Departments to DIS. The first DIS Director was Air Force Brig. Gen. Joseph J. Cappucci, the former Commander of the Air Force Office of Special Investigations.

DIS was limited to conducting investigations within the 50 states, the District of Columbia and Puerto Rico. The agency was organized into 20 districts (19 in the continental U.S. and one in Hawaii) with 243 field units. While DIS investigators were known as special agents, they did not engage in law enforcement activities when the agency was created.

Investigations

DIS activities were confined to conducting DoD personnel security investigations that included national and local agency checks and other investigative inquiries to determine the suitability of military personnel, Government civilian employees, and contractor personnel (when requested by the Defense Industrial Security Clearance Office (DISCO)), for access to classified information. Further investigative inquiries may have involved the resolution of issues such as the existence of criminal records and subversive affiliations.

Since DIS was known within the defense enterprise as a fact-finding agency, at times other defense agencies and military branches requested assistance when investigating a variety of cases.

In 1977, at the direction of the Secretary of Defense, the Special Investigations Center was established within DIS to supervise the conduct of criminal procurement fraud investigations and fraud prevention surveys. This unit eventually became the Defense Criminal Investigative Service in 1981, which is now the criminal investigative arm of the DoD Office of Inspector General.

Upon receiving a request for assistance, the Special Investigations Center reviewed the case file forwarded by the requesting agency. After a thorough review of the exhibits and evidence related to or contained within the case file, the special agents would locate suspects, persons of interests or witnesses in order to question them.

Once the DIS investigation was completed and the special agents exhausted all local leads, the results of the investigation would be passed to the requesting authority who then determined the final and appropriate actions that should be taken.

The subject matters and issues presented in these case files run the gamut from the mundane to the novel, and some cases retain their vividness even after the passage of 30 to 40 years. They also show that despite changes to the original mission of the agency and the PSI program, these case files highlight DSS's rich history, continued support of interagency activities and adaptability to the changing security environment.

The requests for investigative assistance show a variety of topics, including:

- Alleged theft of government items including microwaves, military medical supplies, air conditioners, wrist watches, flying gloves, prescription balance scales, blank checks, death gratuity checks, generators, chain saws, microscopes, tensometers (a device used to measure the amount of stress a material can withstand), Radio Personality Modules test set (a device to increase the strength of a radio signal), calculators, rice, camera and lenses, typewriters, carpet squares and parka liners.
- Sale of cereal packages with military issued markings at a commercial restaurant
- Suspected arson at a Defense Depot
- Vandalism of government vehicles
- Sale of drugs on government premise
- Validity of claims/eligibility under the Civilian Health and Medical Program of the Uniformed Services
- Disbursement of military construction funds without obtaining required approval
- Possible demilitarization violation after the report of an armored vehicle with a mounted 37 mm gun being parked in a driveway
- Research of internal document in order to prepare responses to congressional inquiries
- Unauthorized release of a government audit report by a cleared contractor
- Unauthorized disclosures due to the loss of a notebook containing classified information
- Interviewing persons in connection with sensitive information that appeared in a news article
- Investigation of federal employees reporting to work under the influence of marijuana, other drugs and/or alcohol
- Harassments/threats made to federal employees in retribution for reporting inappropriate behavior
- Monitoring a federal court hearing concerning munitions control violations where a cleared company attempted to export items without an export license authorized by the State Department

DEFENSE INVESTIGATIVE SERVICE:

THE EARLY HISTORY

By Nicole Graham
Office of Public and Legislative Affairs

- Request to assist with the protection of President Nixon during a visit to Macon, Ga.
- Request for possible logistic support by DIS during President Ford's visit to Pittsburgh, Pa.
- Request by the Secretary of the Air Force to provide assistance providing protective services to a distinguished visitor
- Investigations regarding the quality of government-procured food including irregularities in liver packaging and whether the contractor fraudulently switched the quality of liver; the diminished quality of potatoes sold at the Patrick Air Force Base commissary; the loss of oysters due to the lack of refrigeration during transit; pilferage of combat meats from U.S. government shipments; and, allegations that a company altered date codes on milk
- Allegations of fraudulent contractor activity including failure to make equipment for the federal government upon receipt of payment; removing commercial markings and rebranding items by DoD specific source manufacturers; conflict of interest when awarding contracts; preferential treatment in procurement actions; improper relationship between prime and subcontractors; false information reported by contractors such as place of business and requisitions of activity; and, allegations of sexual favors in return for procurement of government contracts.

FIRST CONGRESSIONAL WEBINAR A SUCCESS; COLLABORATION KEY

By Nicole Graham
Office of Public and Legislative Affairs

In order to better share the DSS story with our partners in Congress, the Office of Public and Legislative Affairs (OPLA) invites congressional district staffers to receive an orientation of the DSS mission and operations. These meetings are attended by state and district directors, congressional caseworkers and military liaisons who work directly with constituents and facilities in a Congressional members' state or district.

While these briefings are very informative for the congressional staffers who attend, it also provides OPLA with opportunities to develop and foster relations with staffers working in the local districts.

When determining a location for these events, OPLA considers the number of congressional districts and the number of cleared defense contractors located within the radius of a DSS field office.

Due to the high concentration of cleared facilities located near Huntsville, Ala., OPLA worked with the Southern Region to host a congressional briefing at that field office in late February.

While cleared facilities are highly concentrated in Huntsville, the congressional district offices were more widely dispersed, with some a three-hour drive away. To increase visibility and attendance, OPLA wanted to consider alternatives to 'in person' attendance.

By implementing a new, virtual component to the existing outreach presentation, DSS would be able to efficiently and effectively reach a wider congressional audience while demonstrating the agency's technological capabilities.

Since the Center for Development of Security Excellence (CDSE) has already implemented a webinar program, OPLA discussed the possibility of collaborating with their production team to develop a webinar format that would suit the congressional presentation.

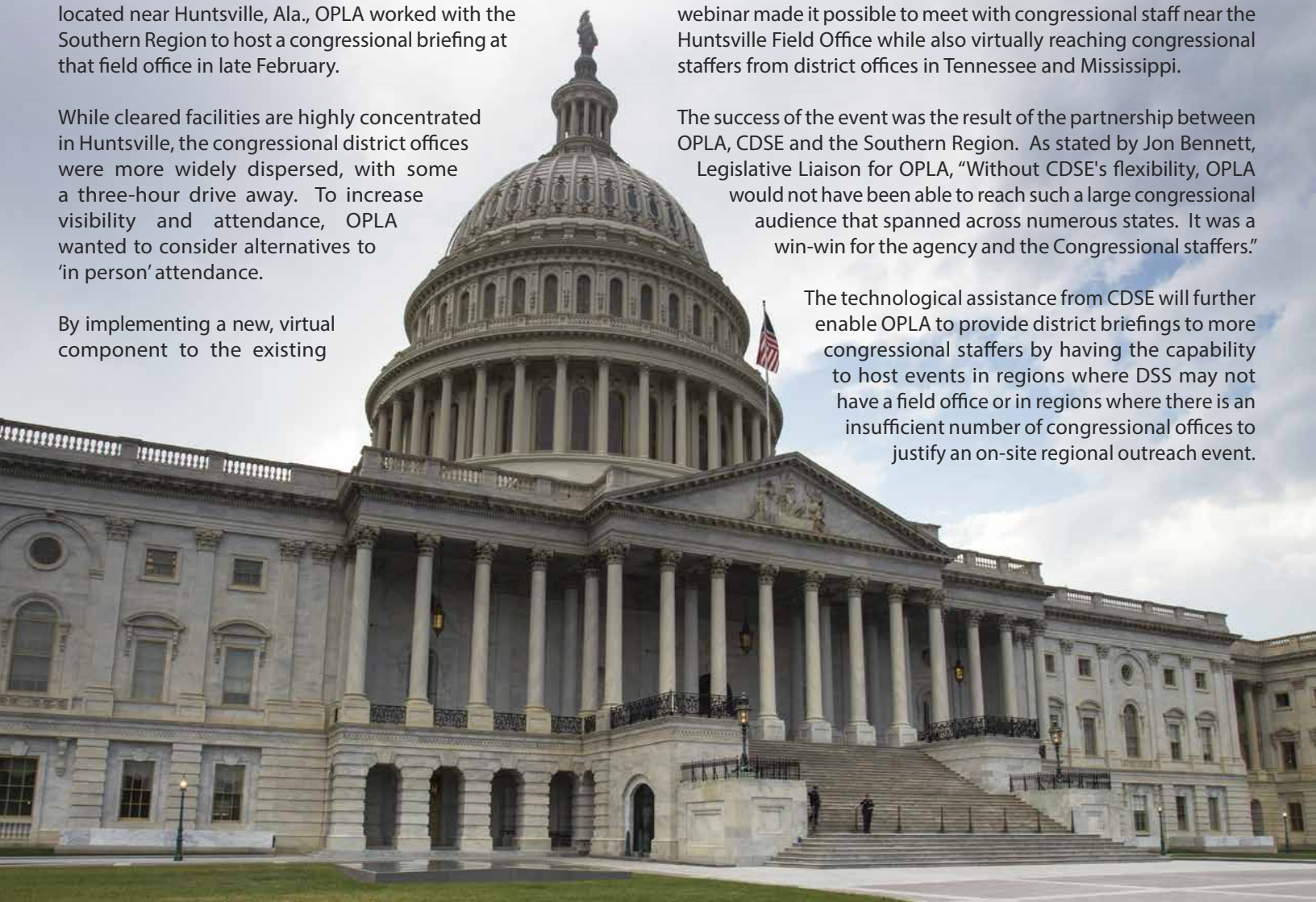
Webinars, or web-based seminars, are a tool DSS uses to address topics and issues of interest that includes an interactive component allowing participants to ask questions while attending a presentation from their desk.

After discussing the objectives and desired format of the webinar, CDSE, OPLA, and the Huntsville Field Office rehearsed the webinar to ensure a smooth operation for the event.

The availability of the webinar nearly doubled the number of congressional staffers who were able to attend the briefing. The webinar made it possible to meet with congressional staff near the Huntsville Field Office while also virtually reaching congressional staffers from district offices in Tennessee and Mississippi.

The success of the event was the result of the partnership between OPLA, CDSE and the Southern Region. As stated by Jon Bennett, Legislative Liaison for OPLA, "Without CDSE's flexibility, OPLA would not have been able to reach such a large congressional audience that spanned across numerous states. It was a win-win for the agency and the Congressional staffers."

The technological assistance from CDSE will further enable OPLA to provide district briefings to more congressional staffers by having the capability to host events in regions where DSS may not have a field office or in regions where there is an insufficient number of congressional offices to justify an on-site regional outreach event.



February Designated CI Awareness Month in Capital Region

In an effort to increase Counterintelligence (CI) reporting and awareness in the Capital Region, Heather Green, Regional Director, and Michael Clapp, Capital Region CI Chief, designated February 2014 as Capital Region CI Awareness Month. The goal of putting CI front and center was to increase both the quantity and quality of reporting from cleared industry, but also ensure that Capital Region staff had the knowledge and skills necessary to recognize and develop issues with a CI nexus.

Over the 28 days in February, the Capital Region staff contacted more than 5,000 cleared facilities through a series of awareness letters. Topics covered in the letters included:

- An introduction to CI Awareness Month
- Suspicious Contact Report development and recognition
- Cyber impact and tools for mitigation
- CI support tools and threat awareness

In addition, the staff coordinated with industry partners to present nine CI awareness briefings at all Industrial Security Awareness Councils (ISAC) held in February within the region. Over 1,500 industry security personnel were reached through these ISAC briefings, presented by region CI special agents and members of the Intelligence Community. Topics covered an array of CI critical aspects from cyber threats to collection and reporting tactics to social engineering awareness.

The internal focus and a key element for the region involved refresher training for Industrial Security Specialists and Information Systems Security Professionals. The training covered the nuances of threat recognition, vulnerabilities and assets, and emphasized the importance of risk management in dealing with cleared industry. The training culminated with a practical exercise in which the Industrial Security Specialists dealt with a potential CI issue that required them to develop a series of questions to gather more information from industry on the potential CI issues. The additional, or even clarified, information could then be submitted to a supporting CI Special Agent as a suspicious contact report.

While the ultimate success of the CI focus during February will be determined in the future, it's clear the effort served to strengthen the DSS /industry partnership and better protect our national interests.

Virginia Beach Field Office Hosts OUSD(I) Visitor

Michael Higgins, Director for Defense Intelligence (Intelligence & Security), visited the Virginia Beach Field Office in late March for an orientation briefing.

"This is the first time Mr. Higgins had visited a DSS field location and he was very impressed with our level of responsibility and how well we are integrated in the field," said Beth Whatley, Virginia Beach Field Office Chief. "Our goal was for him to come away from the visit with a much better appreciation of the scope and breadth of the field's responsibilities, and we count the visit as a success!"

The briefing covered the scope of the workload, outreach activities with industry and government groups, and how the field office [Industrial Security Representatives, Field Counterintelligence and Information Systems Security Professionals] integrate as a team.

The team also briefed on the Counterintelligence Working Group RED DART and attended a RED DART meeting. RED DART stands for Research and Development Defense Alliance of the Research Triangle. It is a unified, cross-agency team of counterintelligence professionals throughout North and South Carolina who are dedicated to the protection of classified and sensitive technology research.

The backbone of the RED DART program is an aggressive and focused CI awareness and education briefing program aimed at cleared contractors in North and South Carolina. The briefing program focuses on bringing real-time, specific, and relevant CI information to those in industry so they can better protect themselves and their intellectual property.

The day ended with a trip to Huntington Ingalls, Inc. (HHI) shipyard in Newport News, Va., where Higgins saw the DSS partnership with industry in action. A team from HHI and DSS provided a joint presentation, which included examples of partnering to protect national security information and a high level overview of the security vulnerability assessment process.

JISAC Draws a Crowd: More Than 600 Attend 18th Annual Event

By Nicole Graham
Office of Public and Legislative Affairs

In late March 2014, the Joint Industrial Security Awareness Council (JISAC) held its 18th annual seminar in Falls Church, Va. More than 600 industry security personnel including Facility Security Officers, Outside Directors, CEOs and many government stakeholders participated in the event.

The JISAC was formed to assist defense contractors in complying with the requirements of the National Industrial Security Program. The council, comprised of seven DSS representatives and 27 industry personnel, demonstrates the continued partnership the agency is forging with industry. Robin Nickel, from the DSS Alexandria Field Office and JISAC chairperson, provided the welcoming remarks.

Annually, the JISAC sponsors a joint event where security professionals from regional industrial security awareness councils, defense contractors and DSS IS Reps can gather and meet to receive information on current security issues.

Other DSS personnel on the JISAC include: Rod Webb, Senior Industrial Security Specialist, and Elizabeth Kim, Industrial Security Specialist, from the Chantilly Field Office; Emily Helstowski and Shelton Mallow, Industrial Security Specialists, from the Alexandria Field Office; and Ursula Stearns, FOCI Operations Division.

Guest speakers for the event included DSS Director Stan Sims; Retired Air Force General Michael Hayden, former director of the National Security Agency; Doug Thomas, Director of Counterintelligence, Lockheed Martin Corporation; Scott Kaine, President, Cyveillance, Inc.; Laura Hickman, Director, DSS Personnel Security Management Office for Industry; Perry Russell-Hunter, Deputy Director, Defense Office Hearings and Appeals; and Micah Komp, DSS Quality Assurance Specialist.

Sims applauded the efforts of the JISAC and stated that "[the council] is the epitome of working together with industry." He provided an update on DSS, to include his priorities for the agency, upcoming challenges, and participated in a question and answer session.

DSS personnel supporting the JISAC include (from left) Elizabeth Kim, Shelton Mallow, Robin Nickel, Rod Webb, Ursula Stearns and Emily Helstowski.

While Sims acknowledged the current efforts to increase industrial reporting, he encouraged all those involved to continue to do better. He further highlighted internal DSS efforts, such as Center for Development of Security Excellence tools and technological advances, to increase the efficiency and ease of communication between the agency and industry.

Presentations by Hayden and Thomas focused on the insider threat, cyber intrusions, and what industry can do to protect against the leak of sensitive information. Both speakers acknowledged that the ever changing security environment creates tough challenges to protect classified and proprietary information; however, continued collaboration between the government and industry will increase the effectiveness of counterintelligence and cybersecurity programs.

Several agencies set up information booths and exhibits, and numerous vendors were on hand to display equipment in support of the December 2013 mandate for electronic fingerprint submissions in support of personnel security clearance investigations.

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.

Andover Field Office Hosts Open House

The Andover Field Office recently hosted a successful open house for cleared contractor security personnel. More than 160 security professionals, representing 90 companies within the Andover area of responsibility including New Hampshire, Maine and six counties in Massachusetts, visited during the open house.

The goal of the event was to foster a partnership with industry, get better acquainted with the Andover industry partners outside the facility environment, introduce these security professionals to the entire field office staff, and showcase recent upgrades to the field office.

Each industry participant received a take-home package of useful information designed to assist them with their security programs. The Andover office plans to make this an annual event.

From the Participants:

"... being an FSO can be a daunting and lonely role in any organization. To be sure, I have had my own 'bumps in the road' as I have executed my responsibilities. It has been a distinct pleasure working with all of the trained and sincere professionals in your organization over the years here. Your team has offered an uncompromised level of support in spite of tremendous schedule demands. I have so appreciated the support and direction as stewards of national defense protected information for our warfighters safety."

"The Open House is a good idea and should continue. It provides the opportunity to talk to staff at all levels in the hierarchy on matters other than your facility assessment. It is a definite step to fostering the concept of a working partnership between industry and DSS. It is also good to be able to put a face to a name. I particularly liked the CD in the exit package. It puts together many of the references I've built over time and will be particularly helpful to new FSOs."

"The event was well orchestrated and so enjoyable. I don't see how you could improve upon it, and it is obvious how much hard work everyone invested into making it a success. ... It was great networking not only with DSS but with other contractors as well. ... I hope we can do it again next year."


DEFENSE SECURITY SERVICE
UNITED STATES OF AMERICA