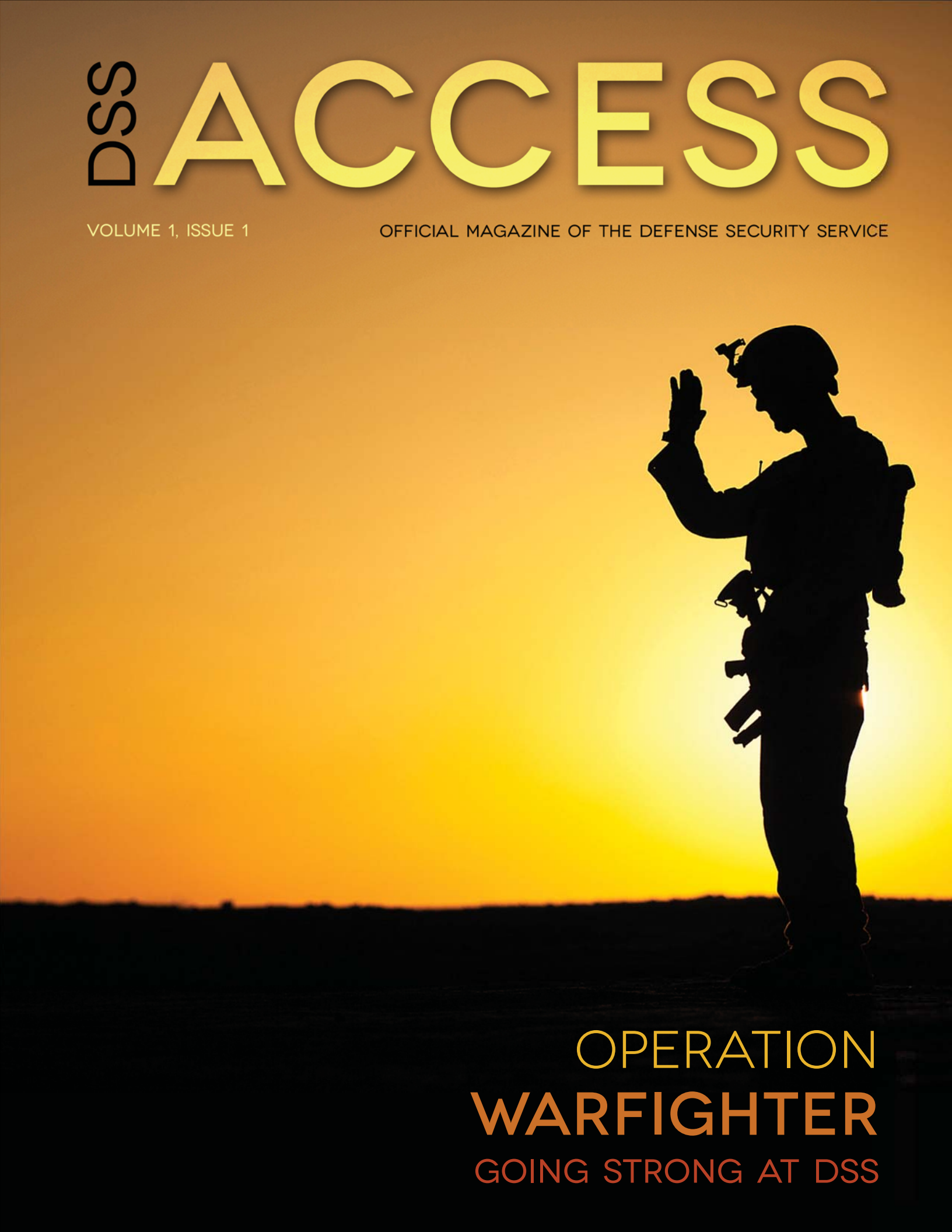
DSS ACCESS

VOLUME 1, ISSUE 1

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE



OPERATION WARFIGHTER

GOING STRONG AT DSS

SPRING 2012

VOLUME 1, ISSUE 1

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

I'm very pleased to introduce the first issue of our new magazine, DSS ACCESS. We chose the name DSS ACCESS to reflect the unique position the Defense Security Service occupies in the National Industrial Security Program. DSS is the link between cleared industry and the U.S. Government. We facilitate the exchange of information, leverage our partnerships, and provide each with ACCESS to the other.

From these pages, we will demonstrate the scope and range of activities in which DSS is involved that make the agency a valued partner. For instance, we present a case study developed internally by the Operations Analysis Group, which provides lessons learned for both DSS and industry to consider. We also share our latest course offerings at the Center for Development of Security Excellence and where we see our efforts moving in the future. We highlight the employees of the Huntsville Field Office. Finally, we recognize our outstanding employees as we present the first team and employee of the year awards.

I want to dedicate this first issue of DSS ACCESS to our motto – "People First, Mission Always." DSS has a diverse, dispersed workforce doing an important mission across the country. We have local field offices and individual employees developing and adopting innovative processes and procedures to get things done. They are working in their communities to enhance the partnership between DSS and our industrial and government partners. In short, we have good people doing good work. Now we can share those successes with the larger DoD security community.

I am excited about this publication. I hope that enthusiasm comes through on these pages and you find relevant, interesting information. Enjoy!

OPERATION WARFIGHTER HAS PLACED MORE THAN 2,000 WOUNDED SERVICE MEMBERS IN INTERNSHIPS WITH MORE THAN 105 DIFFERENT FEDERAL AGENCIES.

(DEPARTMENT OF DEFENSE)

OPERATION WARFIGHTER

GOING STRONG AT DSS

By Valeria Roberts
Human Capital Management Office

On Nov. 9, 2009, President Barack Obama signed Executive Order 13518, Employment of Veterans, which underscores the importance of recruiting and employing veterans, as well as assisting transitioning service members seeking employment in the federal government.

The Defense Security Service (DSS) is actively involved in Operation Warfighter (OWF), one of the programs that falls under the Executive Order.

OWF is an unpaid temporary assignment/internship program for service members convalescing at military treatment facilities. The program provides recuperating service members with meaningful activity outside of the hospital environment, and offers a formal means of transition to the military or civilian workforce.

The program also offers managers the opportunity to acquire manpower to complete work in the office, while giving injured service members a chance to develop new skills during the temporary assignment and a focus on future possibilities. The OWF program at DSS is managed by the Human Capital Management Office (HCMO).

The Capital Region was the first DSS office to benefit from the capabilities of an OWF intern and continues to lead the agency in supporting the program. Army Chief Warrant Officer Rendell Long was the first intern hired under the program and served as an Industrial Security Specialist in early FY11. Since then, the Region has worked with four additional interns and is looking to add even more.

With little guidance on hosting an OWF intern, Regional Director Chris Forrest modeled a work plan that mirrored the Student Internship Program, because the goals were similar; "getting them ready for employment in civilian service or industry." His work plan has been adopted across the region.

Sharon Dondlinger, Crystal City Field Office Chief, is currently working with an OWF intern, building on "marketable skill sets and good security credentials" that the wounded warrior can use to transition to his civilian job in Texas, where he works in the field of criminal justice.

When asked about challenges he faced in completing his DSS duties, Dondlinger said, "He sustained some injuries

APPROXIMATELY 350 SERVICE MEMBERS HAVE TRANSITIONED INTO FEDERAL JOBS AS A RESULT OF OPERATION WARFIGHTER

DSS employees participated in the Walter Reed National Medical Center Mini Wounded Warrior Career Fair in Bethesda, Md., on Jan. 19, 2012. From left, Robin Nickel, DSS Industrial Security Representative from the Alexandria Field Office; Patrick Brick, DoD OWF Program Manager; Torland Wingfield, Office of the Director of National Intelligence Outreach and Recruitment; and Izzy Sanchez, DSS Recruitment Officer (front).

where a lot of walking may be painful, but he isn't afraid to say when it starts to hurt and we are cognizant of that… so we take him to a facility that isn't large, close to the Metro and has on-site parking."

The most recent OWF intern is Army Sgt. Emily Moore, who works under the supervision of Horace Russell, Office of the Chief Information Officer (OCIO).

Moore, who is a helicopter mechanic, plans to transition into the civilian or private sector in the field of information technology (IT). In her internship, she supports the OCIO IT Help Desk, which in turn supports her Certified Information Systems Security Professional (CISSP) training requirement.

Russell believes the internship is both beneficial to DSS and helps prepare Moore for her future career in IT. He contends that one of the keys to the success of Moore's internship is that she was paired with an individual who had prior Air Force service, and they quickly established a great working bond.

Operation Warfighter strives to demonstrate to participants that the skills they have obtained in the military are transferable to civilian employment.

It also enables federal employers to better familiarize themselves with the skill sets and challenges of wounded, ill and injured service members, as well as benefit from the talent and dedication of these service members.

One goal of the OWF program then is to transition the wounded warrior into a job working with the Department of Defense. Christopher Veade, a security investigator/analyst, is one such individual who interned with DSS

OPERATION WARFIGHTER ACROSS DSS

DIRECTORATE	INTERNSHIP GOAL	LOCATIONS
Center for Development of Security Excellence	5	Linthicum, Md.
Counterintelligence	2-3	San Diego, Calif., Boston, Mass., Irving, Texas and Washington, DC
Equal Employment Opportunity	1	Quantico, Va.
Foreign Ownership Control or Influence	1-2	Quantico, Va.
Industrial Security Field Operations (Headquarters)	5	Quantico, Va.; Fort Meade, Md.; Alexandria, Va.
Capital Region	2	Alexandria, Va.
Northern Region	3	St. Louis, Mo., Chicago, Ill., possibly Minneapolis, Minn.
Office of the Chief Information Officer	1	Fort Meade, Md.

under the OWF Program and is now supporting the agency as a defense contractor.

Veade, who received a medical discharge from the Marine Corps, served as an Industrial Security Field Operations staff action officer under the supervision of Sharon Bickmore, Assistant Director for Operations, when he was an OWF intern.

"He came in and hit the ground running, and made a direct contribution to our National Industrial Security Program," said Bickmore. She attributes Veade's success to having a mentor (Darnell Carlisle), who ensured he had an understanding of the DSS mission and background.

Veade agrees. "There was an instant connection," he said. "Darnell Carlisle is retired Army and helped me out a lot – not just looking for a job at DSS but elsewhere. He gave me a lot of good advice."

DSS leadership has fully embraced the OWF Program, and managers have committed to offering 20 to 22 internships during FY12 – an increase of 10 slots from the previous year.

As DSS participation in the OWF internship program increases in the National Capital Region, Field Offices across the country have expressed interest in the program. HCMO is reaching out to the Veterans Administration for assistance in reaching disabled veterans who are interested in participating in an unpaid internship.

Partnering with other agencies and support of the DSS leadership are two reasons the DSS OWF program is such a success. Perseverance has paid off and DSS is on the move reaching out to service members seeking internship opportunities that can prepare them for jobs with the federal government or industry.

FROM LEFT: Brett Lambert, Deputy Assistant Secretary of Defense for Manufacturing & Industrial Base Policy OUSD (AT&L); Dale Hamby

ANNUAL FOCI CONFERENCE

By Steve Lindquist
Industrial Policy and Programs

The Defense Security Service held its annual Foreign Ownership, Control or Influence (FOCI) Conference in November 2011, for companies operating under DSS FOCI mitigation. The event was designed for two audiences; day one for Outside Directors and Proxy Holders, and day two for Facility Security Officers (FSO).

DSS established this event to help educate industry's Outside Director, Proxy Holder and FSO communities on current DSS and FOCI related issues, as well as provide a forum for contractor input regarding the DSS FOCI mitigation and oversight program.

The conference opened with DSS Director Stan Sims welcoming attendees, and presenting an overview of the current state of DSS and his vision for the future of the agency. The keynote speaker, Brett Lambert, Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy, Office of the Under Secretary of Defense (Acquisition, Technology and Logistics), shared his perspectives on foreign investment in the defense industrial base and the current challenges facing DoD in the globalized market.

"Foreign investments are becoming increasingly more globalized, more commercialized and more financially complex" said Lambert.

Later in the day, The Honorable Michael Oxley, a current Proxy Holder and co-author of the Sarbanes-Oxley Act of 2002, discussed and answered questions regarding corporate governance within the role of Corporate Board members; specifically the importance of public board financial transparency as it relates to risks and controls outlined in the Sarbanes-Oxley Act. The Act set new and enhanced standards for all U.S. public company boards, management and public accounting firms, and addresses corporate accountability and responsibility.

Other presentations offered by DSS subject matter experts featured topics such as FOCI Oversight, Cybersecurity, and Counterintelligence. To close out the first day, a panel of DSS experts fielded questions from the audience. Many of the topics presented by DSS on the first day of the conference were also presented on the second day for the FSOs.

FOCI Program Analyst; Ben Richardson, Chief, FOCI Operations Division; and Justin Walsh, FOCI Program Manager. *Photos by Derik Bland.*

EXPANDS TO INCLUDE FSOS

"FOREIGN INVESTMENTS ARE BECOMING INCREASINGLY GLOBALIZED, COMMERCIALIZED AND FINANCIALLY COMPLEX"

KEYNOTE SPEAKER BRETT LAMBERT

In addition, Martin Faga, former CEO of MITRE Corporation and current Outside Director and Proxy Holder, spoke on the relationship between the FSOs and the Outside Directors and Proxy Holders. Faga commented on the importance of teamwork between the FSOs and the Government Security Committee, emphasizing how they must work in tangent to ensure compliance in their mitigation agreements.

At the end of the day, three industry FSOs – Jennifer Brown with iDirect Technologies, Dennis Burnett with EADs North America, Inc., and Daniel Crosby with DRS Technologies – participated in a panel and answered questions regarding best practices for FSOs under DSS FOCI mitigation. During the panel session an audience member asked how a new company and a new corporate FSO should grow their staffs. Crosby responded by discussing the importance of establishing internal standards and having regular meetings with all facility FSOs to ensure consistency across the facilities.

In all, more than 300 Outside Directors, Proxy Holders and FSOs attended this event. Many of the Outside Directors and Proxy Holders are retired flag officers and former senior government officials. This annual event, which launched in 1989, was originally set for one day for only Outside Directors and Proxy Holders. In 2010, DSS hosted the first FSO conference. Based on feedback from the FSO community, DSS has decided to make their involvement an annual event.

DSS has tentatively scheduled the 2012 conference for late October or early November. Attendance will once again be for Proxy Holder, Outside Directors, and FSOs for companies that are under current FOCI mitigation with DSS. For more information regarding the DSS FOCI program, please visit the dss.mil website at http://www.dss.mil/isp/foci/foci_info.html.

CERTIFICATION & ACCREDITATION
PILOT COURSE TAKES OFF

Given the persistent cyber threat posed to industry, it benefits both the Defense Security Service (DSS) and industry for Industrial Security Representatives to have a technical knowledge of information technology at contractor facilities.

In addition, DSS determined a need for individuals trained in certification and accreditation to supplement Information Systems Security Professionals (ISSPs) in the field.

To meet the need, the Office of the Designated Approving Authority (ODAA) partnered with the Center for the Development of Security Excellence (CDSE) to develop a Certification and Accreditation (C&A) Course for DSS employees. The pilot for the course was conducted recently at the Russell Knox Building at Quantico, Va.

The training provides additional technical knowledge and skills and is available to Industrial Security Representatives from across the country who have completed the course prerequisites.

ODAA provided three Certified ISSPs as instructors for the pilot: Tracy Brown, David Scott and Ryan Gindhart. Deborah Hutchins and Manoharan Krishnan, also of ODAA, supported exercises and role playing activities. Rojohn Soriano and Steve Raymond from CDSE hosted and led instruction for the class. An estimated two dozen students should complete the course over the next year.

This multifaceted training curriculum includes role playing, hands on activity, instructor-led lectures and real world support from ISSPs.

Students who complete the training and pass a comprehensive examination, receive a certificate from the DSS Designated Approval Authority, Randall Riley. They also ensure a cadre of leaders, trained across disciplines, to assist in C&A activities.

The students completing the first course were: Adrianne Backhus, Crystal City Field Office; Lisa Dearmin, Cyprus Field Office; Harry Kurtz, Philadelphia Field Office; Richard Noe, Philadelphia Field Office; Roy Parker, Virginia Beach Field Office; John Skinner, Crystal City Field Office; and, Kerry Waldrip, St. Louis Field Office.

The next C&A Reviewer Class is tentatively scheduled for June 2012 at Quantico.

FROM TOP: From left, Harry Kurtz, Roy Parker and Richard Noe review the board of questions during a learning exercise. David Scott (left), and Rojohn Soriano review student test papers. Lisa Dearmin and John Skinner listen to lecture. *Photos by Hollie Rawl*

OVERSIGHT VERIFICATION PROCEDURES: SAPS CAN CAUSE CONFUSION

As a Facility Security Officer (FSO), have you ever had to inform your DSS representative that DSS did not have cognizance over an area or room at your facility? Did you deny your DSS representative entry to an area that was performing on a U.S. Government classified contract? Did you deny the DSS representative access to the DD Form 254, Contract Security Classification Specification because you did not know if he/she possessed the required access? If so, you have been involved in a government oversight verification situation.

As we all know, DSS is responsible for security oversight of Defense classified contracts in industry to include Special Access Program (SAP) contracts. When a SAP is established, the Deputy Secretary of Defense decides whether to have industrial security oversight responsibilities remain with DSS or to carve DSS out of these responsibilities. When the Deputy Secretary of Defense "carves-out" DSS from industrial security responsibilities of a SAP it is referred to as a "carve-out SAP."

Additionally, DSS is not responsible for classified contracts for agencies that have not entered into agreements with the Secretary of Defense as the executive agent for the National Industrial Security Program. Lastly, DSS is not normally the Cognizant Security Office (CSO) for Secure Compartmented Information (SCI) contracts. All of the aforementioned contracts can pose a problem for the FSO and DSS representative.

The mere existence of a SAP, SCI, or other classified contracts for which DSS is not the CSO might be classified. These contracts might also contain special handling caveats. These situations result in the FSO being reluctant to provide DSS representatives with contract information when answering questions concerning the special activity.

The FSO and DSS representative must be very careful when verifying government oversight of an area or room at a cleared contractor. Discussing the fact that a special classified contract exists or possibly exists at a contractor location over unclassified e-mail or non-secure telephone might unintentionally disclose classified information and put national security at risk.

DSS personnel are instructed to take the actions listed below to confirm government oversight of a classified contract for which DSS is not the CSO:

- Request a copy of the DD Form 254. Indication of the government security oversight responsibility and government customer should be referenced on the form. The form should be countersigned by the government security officer.

- If the DD Form 254 is not available or at a handling caveat that excludes access, coordinate contacting the government customer with the FSO while at the facility. Oversight should be verified with the government security officer, not the government Contracting Officer.

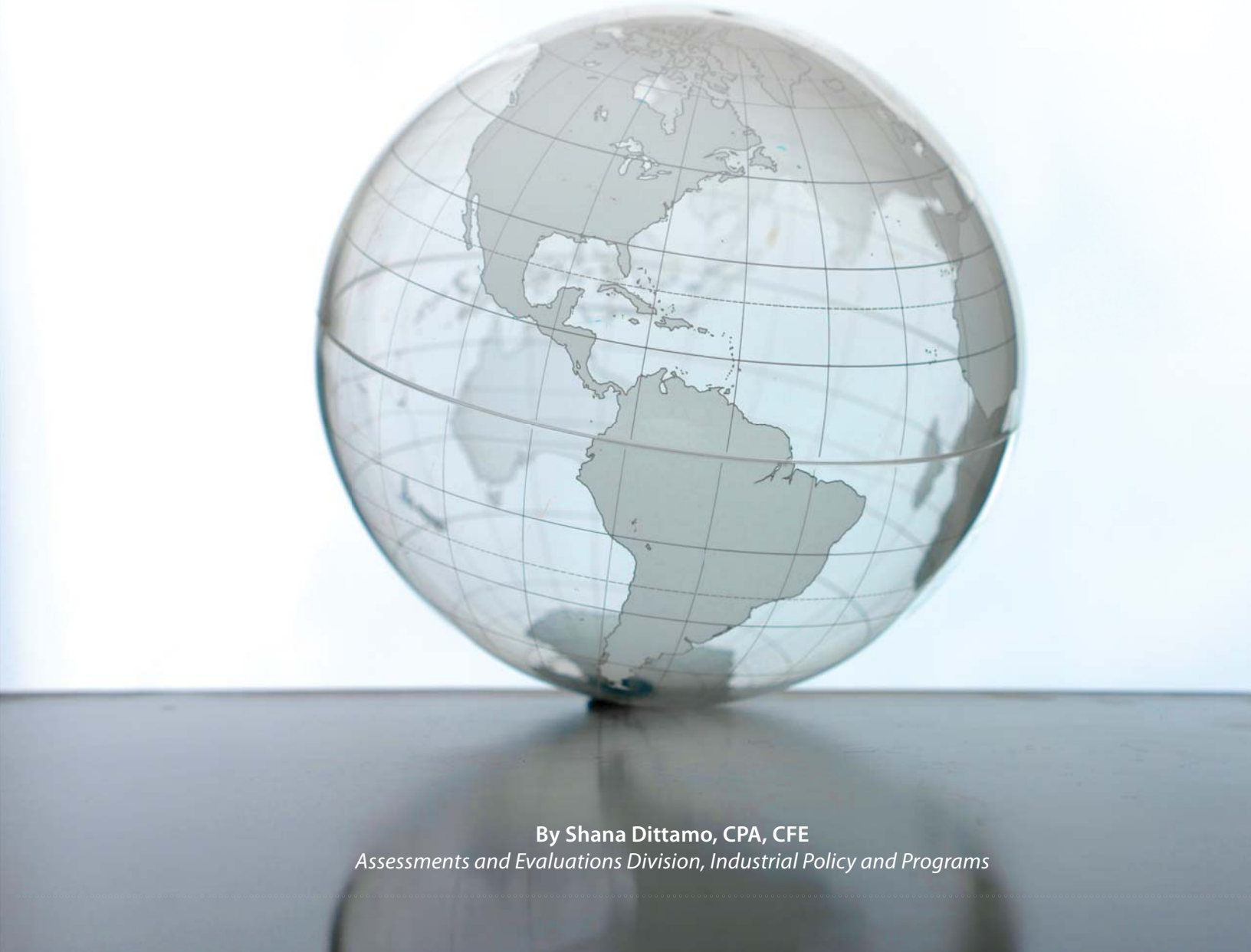
- If verification is unsuccessful using the methods above, the FSO should contact the government customer (security officer) and have the government customer contact DSS Headquarters to verify government security oversight.

DSS is concerned when excluded from or denied access to an area or room at a cleared contractor location. In this case, DSS personnel are required to verify government oversight of the classified contract; not gain access to the classified contract or area.

The role of the FSO is vital to national security. DSS is working within the Department of Defense as well as external organizations to streamline the process for verifying government oversight of classified contracts in which DSS is not the CSO. Until this is resolved, FSOs will have an important role ensuring proper oversight is provided for their facility.

The DSS Headquarters point of contact for confirming other government oversight at industrial facilities is the DSS Special Access Programs Office, at (571) 305-6351.

UNMASKING
FOREIGN OWNERSHIP, CONTROL OR INFLUENCE
CONCEALED IN COMPLEX FINANCIAL STRUCTURES



By Shana Dittamo, CPA, CFE
Assessments and Evaluations Division, Industrial Policy and Programs

The globalization of the economic market has resulted in a spider web of complex financial mechanisms, which can mask foreign influence on cleared companies. DSS is looking at these intricate instruments to detect foreign ownership, control and influence over National Industrial Security Program (NISP) classified contracts.

According to the Bureau of Economic Analysis, the United States received $236 billion in Foreign Direct Investment (FDI) in 2010. This constitutes over 16 percent of the United States Gross Domestic Product. The Assessments & Evaluations (A&E) Division, of DSS Industrial Policy and Programs, reviews direct and indirect investment in NISP companies from numerous foreign nations to include India, China, United Arab Emirates, and the United Kingdom.

Ownership in publicly traded companies and corporations has traditionally been direct and transparent. Stock is purchased on an exchange and the ownership is equal to the percent of stock owned. The Securities and Exchange Commission's (SEC) mission is to protect investors, maintain fair, orderly and efficient markets, and facilitate capital formation. Therefore, the SEC requires extensive disclosures from publicly traded companies to include management composition and changes, financial posture, and anticipated mergers and divestitures.

Additionally, when an entity (person or company) buys more than five percent of a publicly traded company's stock, the company is required to disclose the ownership change. The disclosure requirements, coupled with the SEC's EDGAR database, provide a clear window to the ownership and management structure of the company.

An increasingly popular method of buying into a company though is through indirect investment. Indirect investment vehicles can include hedge funds, private equity firms, venture capital funds and sovereign wealth funds (SWFs). These privately held entities do not have the same disclosure requirements as publicly held companies and function with the mystique of a black box.

The nebulous nature of indirect investment vehicles is attractive to those wishing to own or control a company, yet enjoy immunity from regulatory disclosure requirements. Further, the method in which financial instruments are structured can pose a challenge to transparency.

High risk derivatives and other exotic types of accounts further complicate the indirect investment landscape.

[INDIRECT INVESTMENTS] DO NOT HAVE THE SAME DISCLOSURE REQUIREMENTS AS PUBLICLY HELD COMPANIES AND FUNCTION WITH THE MYSTIQUE OF A BLACK BOX.

For example, hedge funds are made more opaque by accounts called side pockets. Side pockets are segregated accounts that hedge fund managers use for thinly traded investments and are tracked separately from the liquid assets. As asset structures gain increasing complexity, ownership becomes more difficult to identify.

The lack of transparency and opaqueness of private equity funds makes them an attractive investment vehicle for sovereign wealth funds. SWFs are government-owned and controlled pools of capital that are invested in various financial assets. Typically, the capital is generated from the nation's budgetary surplus.

The Department of the Treasury estimates that there are over 50 SWFs controlling more than $3 trillion in assets. Among the largest SWFs in the world are the Abu Dhabi Investment Authority which has an estimated value of $627 billion, and the China Investment Corporation worth approximately $400 billion. Foreign influence and control can be camouflaged by channeling SWF money through private equity funds which consequently poses a threat to our national security.

The A&E Division is working to reduce the vulnerability of NISP facilities' exposure to foreign influence and control. By mapping the organizational structures of companies and data mining numerous databanks, DSS is increasing its ability to unearth the veiled nature of private companies and mitigate the threat of foreign control or influence.

THE UNDISCLOSED "SIDE TRIP"

EVENT DETAILS

In January 2009, a cleared contractor employee (Subject) who was a dual citizen, volunteered to swear his allegiance to the United States and destroy his country of origin passport to be eligible for a security clearance. These actions provided sufficient mitigation and he was adjudicated favorably for a Secret personnel security clearance eligibility.

In September/October of 2010, the Subject traveled overseas on a classified program-related business trip. Upon his return, he completed his company's mandatory travel debriefing and indicated "nothing unusual occurred." A few weeks later, the Subject amended his report at his supervisor's direction, indicating a "side trip" to his country of origin to see his ailing father.

The Subject's supervisor was made aware of the "side trip" after the Subject had completed the initial debriefing. The supervisor directed the Subject to contact his Facility Security Officer (FSO) concerning the side trip.

In mid-November 2010, the Subject's company submitted a suspicious contact report (SCR) to DSS outlining the Subject's travel. The SCR was entered into DSS' system of record and forwarded to the DSS Operations Analysis Group.

By forwarding the SCR to DSS, the company believed they met the reporting requirements and did not enter an adverse information report into the Joint Personnel Adjudication System (JPAS) on the Subject. While it is not a National Industrial Security Program Operating Manual (NISPOM) requirement for FSOs to enter an adverse information report in this instance, self-reporting of foreign travel is required on an SF-86 Questionnaire for National Security Positions.

The company responded immediately when asked by DSS to follow-up with a JPAS entry on the Subject. In early 2011, DSS suspended the Subject's eligibility for access to classified information based on the suspicious nature of the trip, the country visited (an embargoed country), and the failure to report the trip deviation until prompted by his supervisor.

DSS requested the Office of Personnel Management conduct a Reimbursable Suitability Investigation (RSI) on the subject based on this incident. At the same time, the company's FSO interviewed the Subject in order to obtain more information concerning his actions. The Subject provided the following information:

- Subject's father is a U.S. citizen who returned to their country of origin to attend his daughter's funeral
- Subject's father had not returned to the United States since the funeral
- Subject stated while in the country the business trip was taking place, he applied for, and obtained, a Visa to enter his country of origin
- Subject stated he used his U.S. passport to enter his country of origin, was not in possession of a foreign issued passport, and had no issues entering or exiting his country of origin
- Subject reported he had his company issued laptop and Blackberry in his possession

An internal investigation conducted by the company revealed the following:

- The company's Export Compliance team indicated there was definitive proof that "an engineer [Subject] with a company-issued laptop and Blackberry went to a unauthorized country, with company assets and presumably International Traffic in Arms (ITAR) data"
- An engineer traveling overseas supporting the program in question with a laptop is fairly certain to be in possession of export-controlled data and documents
- Based on these findings, the company was required to file a voluntary disclosure with the U.S. State Department
- As part of the Export Control review by the company of this incident, the Subject revealed he did have a foreign passport from his country of origin
- Subject revealed that he applied for and received this passport approximately two months after he destroyed his original passport in January 2009

TIMELY REPORTING

In this case, it took more than two months from receipt of the SCR for DSS to take action on Subject's clearance eligibility. This case highlights the need for companies to report incidents in a timely fashion and, conversely, DSS' need to respond and take action more quickly.

LESSONS LEARNED

Given the suspicious nature of the trip, potential espionage indicators, the embargoed country visited, and the failure to report the trip deviation, DSS should have taken more timely action.

Further, the circumstances should have warranted the immediate suspension of the Subject's access to classified information by the FSO and resulted in an adverse information report in JPAS.

Once the Subject's travel deviation was known, the FSO should have promptly interviewed the subject to determine the basic facts of the trip. A complete adverse information report in this case would have included more information, for instance, how the Subject entered the country of origin, whether or not the Subject took his company laptop and Blackberry with him, if the subject volunteered for or "invited himself" on the trip, and whether there were other company employees on the trip who may have known about the travel.

The export violation also highlights the need for regular security education and foreign travel briefings to help identify potential issues.

OUTCOMES

As a result of the company's internal investigation, the Subject was separated from employment. DSS entered a Loss of Jurisdiction and the Subject has an unresolved incident report on file in JPAS.

The case was forwarded to federal law enforcement for further review.

William Stephens (right), Director, Counterintelligence Directorate, presents Huntsville Field CI Specialist Joe Parker with the award for Counterintelligence Collector of the Year.

HUNTSVILLE FIELD OFFICE EMPHASIZES **PROFESSIONAL DEVELOPMENT & OUTREACH**

By Sara Ballard
Senior Industrial Security Representative
Huntsville Field Office

The Huntsville Field Office, nestled in the heart of Alabama's "Rocket City," home of Redstone Arsenal, continues to thrive in advancing the professional development of employees. It has also embraced the agency's philosophy of "telling the DSS story" at each opportunity or interaction with industry and government stakeholders.

Industrial Security Representatives Sara Ballard and Elsa Nylander successfully completed the requirements for the Security Fundamentals Professional Certification (SFPC). The SFPC is the first of four certifications within the Security Professional Education Development Program (SPēD).

The SFPC is a measure of a security practitioner's understanding of facts, concepts, and principles the DoD security community deems critical to successfully perform functions, implement programs, and pursue missions necessary to manage risks to and protect DoD assets.

Stan Sims, DSS Director, has emphasized the importance

[THE HUNTSVILLE FIELD OFFICE] HAS ALSO EMBRACED THE AGENCY'S PHILOSOPHY OF "TELLING THE DSS STORY" AT EACH OPPORTUNITY OR INTERACTION WITH INDUSTRY AND GOVERNMENT STAKEHOLDERS.

THE HUNTSVILLE FIELD OFFICE IS NESTLED IN THE HEART OF ALABAMA'S "ROCKET CITY," HOME OF REDSTONE ARSENAL.

of the program and the importance of holding DSS professionals to the same high standards as the rest of the Department.

Field Office personnel supported the annual local NCMS Luncheon in December. Senior Industrial Security Representative Jeannie Russell and Industrial Security Representative Jason Duquette, supported by other ISRs from the office, presented an overview of the Security Rating Matrix to an audience of approximately 150 Industrial Security professionals. The briefing provided clarity for those security professionals that had not yet experienced a DSS assessment using the matrix.

Field Counterintelligence Specialist Joe Parker was named the Counterintelligence Collector of the Year by the Counterintelligence (CI) Directorate. Bill Stephens, Director CI, visited Huntsville in January to present the award.

During the presentation, Stephens stated that the selection criterion for this award is quite stringent, and that FCIS Parker's selection was well deserved.

GRADUATE LEVEL COURSES ARRIVE AT CDSE

Security as an Integral Part of DoD Programs

Provides a strategic perspective on the function of security across disciplines and DoD organizations.

Organizational Considerations in Applying Security within the Federal and DoD Bureaucracy

Presents an in-depth look at how to work within the Federal and DoD bureaucracy to accomplish security missions and objectives.

Constitutional Law and its Application to DoD Security

Examines the origins of, distribution of, and limitations upon governmental authority under the Constitution of the United States and how DoD security programs and policy are shaped by case law.

Understanding Adversaries and Threats to the United States and DoD

Addresses the intentions and capabilities of the three to five most significant adversaries to the United States and DoD; also examines the multifaceted concept of threat.

Statutory, Legal, and Regulatory Basis of DoD Security Programs

Presents the specific statutes, regulations, and Executive Orders driving the establishment and implementation of DoD and Federal security programs.

The Center for Development of Security Excellence (CDSE) is offering five more courses in their graduate-level curriculum, now available for enrollment.

While the workload of each course is equivalent to a graduate-level college course, no degree is necessary and no tuition is required.

The courses are a blend of online and instructor-led learning. While most classes are asynchronous (any time), there will be scheduled synchronous (real-time) sessions.

All classes will be recorded and made available for absentees. The course sessions span 16 to 17 weeks and course work will be graded.

These five courses, along with "Challenges in Analyzing and Managing Risk," will be included in CDSE's planned curriculum of approximately 16 courses. ("Challenges in Analyzing and Managing Risk" is currently being taught and another course will be available in May).

The curriculum is designed to support leaders in the security community who intend to pursue SPēD Security Program Integration Professional Certification.

To enroll, a student must:

- Be a Federal Government employee or a Military Service member;
- Hold a SPēD Security Fundamentals Professional Certification (SFPC);
- Have Agency recommendation; and
- Hold a SECRET Clearance eligibility.

Interested students can register through STEPP at: https://stepp.dss.mil/SelfRegistration/Login.aspx

>> SPECIAL RECOGNITION

CDSE TRAINING RAKES IN AWARDS

The DSS Counterintelligence (CI) Directorate and DSS Center for Development of Security Excellence (CDSE) developed the "Thwarting the Enemy: Providing Counterintelligence and Threat Awareness to the Defense Industrial Base" course to reach employees at the 13,000 plus cleared contractor facilities across the United States with training that emphasizes the foreign collection threat targeting U.S. critical technologies and their requirement to report those suspicious contacts.

In its first year, the "Thwarting the Enemy" course has had over 40,000 course completions and has been recognized with five awards.

The course received the Defense Intelligence Agency's coveted "Annual Defense Counterintelligence and Human Intelligence Award," for CI Training and Education for 2010.

Excerpts from the citation read: "The web-based training epitomized its dedication and commitment to improving counterintelligence support to the Department of Defense and national security and strengthening collaborative efforts within the intelligence and law enforcement communities. Its achievements increased overall understanding of the complex threat environment and the threat to United States technologies resident in cleared industry, and ultimately improved the effectiveness of counterintelligence support to investigations and operations."

The course also won a Silver Horizon Award in the categories of government and educational products. The Horizon Interactive Awards is a prestigious international, interactive media awards competition recognizing the best websites, video, print and interactive media. Winning entries are dubbed the "best of the best" in the interactive media industry.

And finally, the course won a Gold Omni Award in the categories of government and educational products. The Omni Inter-media Award is an international award recognizing outstanding television, video, film, internet, interactive, audio & animation productions.

The course can be accessed at https://cdsetrain.dtic.mil/thwarting/

Annual Defense Counterintelligence and Human Intelligence Award for CI Training and Education

HORIZON INTERACTIVE AWARDS

Silver Horizon Award in the categories of government and educational products

Gold Omni Award in the categories of government and educational products

FACILITY SECURITY OFFICER CURRICULUM TRANSITION COMPLETE

During FY11, the Center for Development of Security Excellence (CDSE) revised the Facility Security Officer (FSO) curriculum by eliminating the Essentials of Industrial Security Management (EISM) Course and replacing it with a suite of 11 online courses.

Students enrolled in EISM as of Sept. 30, 2011, were given 90 days to complete and receive credit for this course. Students who could not complete the EISM within those 90 days are required to complete the replacement suite of courses. The courses listed below supersede those listed in ISL 2010-01, Article 4.

EISM has been replaced with the following 11 courses:

- Introduction to Information Security (IS011.16)
- Industrial Security Facilities Database (ISFD) Facility Clearance Verification and Notifications for Industry v3 (IS113.06)
- Personnel Clearances in the NISP (IS142.16)
- JPAS/JCAVS Virtual Training for Security Professionals (PS123.16)
- Developing a Security Education Program (GS104.16)
- Understanding FOCI Basics (IS065.16)
- Integrating CI and Threat Awareness into your Security Program (CI010.16)
- Facility Clearances in the NISP (IS140.16)
- NISP Reporting Requirements (IS150.16)
- Visits/Meetings in the NISP (IS105.16)
- NISP Self Inspections (IS130.16)

CDSE completed the transition of the FSO Program Management Curriculum for Possessing Facilities and the FSO Orientation Curriculum for Non-Possessing Facilities.

Both curricula comply with the training requirements stated in National Industrial Security Program Operating Manual (NISPOM) paragraph 3-102.

Successful completion of any of the previous versions of required NISPOM FSO training satisfies the current NISPOM FSO training requirement unless advised otherwise by a DSS IS Rep.

NEW FSO Program Management Curriculum for Possessing Facilities

- FSO Role in the NISP (IS021.06)
- EISM replacement courses
- Safeguarding Classified Information in the NISP (IS109.16)
- Derivative Classification (IF103.06)
- Marking Classified Information (IF105.16)
- Transmission and Transportation for Industry (IS107.16)

NEW FSO Orientation Curriculum for Non-Possessing Facilities

- FSO Role in the NISP (IS021.16)
- EISM replacement courses

These curricula are provided by CDSE and are available at http://go.usa.gov/BEL

CDSE INTRODUCES SECURITY SHORTS

Recognizing the time demands all security professionals face, the Center for Development of Security Excellence (CDSE) is producing short training videos that are usually 10 minutes or less. These "Security Shorts" allow security professionals to refresh their knowledge of a critical topic or quickly access information needed to complete a job. CDSE plans to develop additional "Security Shorts" in FY12.

In 2011, CDSE released six Security Shorts:

Counterintelligence Concerns for National Security Adjudicators

Provides learners an opportunity to practice recognition of counterintelligence concerns relevant to the performance of their job tasks and raises awareness of these issues and their importance in the context of the adjudication process.

Classified Storage Requirements

Learners receive a refresher course on requirements and best practices for storing classified information and complete exercises applying this knowledge.

Special Access Program (SAP) Security Incidents

Allows learners to practice categorizing SAP security incidents and choose the best actions to take in response.

Business Structures - KMP: To Clear or Not to Clear

Provided learners an opportunity to practice identifying Key Management Personnel (KMP) in different business structures. Reinforces information taught in a web-based prerequisite to the Fundamentals of Industrial Security Level 2 Course (FISL 2).

Antiterrorism Force Protection

Learners received a refresher course on the four DoD Threat Levels and five Force Protection Condition (FPCON) levels. The training provides learners an opportunity to see some of the typical FPCON security measures employed in various contexts.

You're a New FSO: Now What?

Provides newly appointed FSOs a high-level overview of their responsibilities, guides them to essential resources, and introduces the CDSE Facility Security Officer (FSO) training curricula (a suite of 16 web-based courses for possessing facilities and a suite of 12 web-based courses for non-possessing facilities).

See the CDSE "Security Shorts" at http://www.dss.mil/cdse/shorts

2011 DSS Team of the Year is the BRAC Program Management Office, from left, Tom Xenakis, Nicole Rhodes, Nancy Riggins, and Tom Lewis. The Director Awards are presented to those who exhibit the highest standards of excellence.

DSS RECOGNIZES EMPLOYEE &

At the first Director Award Ceremony in February 2012, DSS Director Stan Sims recognized the recipients of the DSS Employee of the 4th Quarter, Employee of the Year and Team of the Year awards.

Andrew Woods, DSS Counterintelligence Directorate, was named the Employee of the 4th Quarter and 2011 Employee of the Year; and the Base Realignment and Closure (BRAC) Program Management Office was selected as the 2011 Team of the Year.

The Director Awards are presented to those who exhibit the highest standards of excellence, dedication, and accomplishment in support of advancing the agency's mission. There are two categories for which an employee or team is nominated for the Director Award – Business Results or Agency Core Values. Business Results considers factors such as: Building partnerships, innovation, customer focus, and process improvement. Agency Core Values considers such factors as: Dependability, respect, integrity, agility, collaboration, and accountability.

In selecting the Employee of the Year awardee, each Employee of the Quarter recipient for the 2011 award period was considered.

Competing for the Employee of the Year award were Woods, and Marlena Nisbet, Defense Industrial Security Clearance Office, Industrial Security Field Operations, selected as the Employee of the 3rd Quarter.

[ANDREW WOODS] HAS ESTABLISHED PARTNERSHIPS THAT INTEGRATE BOTH SERVICE DELIVERY AND POLICY TO BETTER SERVE INTERNAL AND EXTERNAL CUSTOMERS, AND ENSURE STAKEHOLDERS HAVE ACCESS TO RESOURCES NECESSARY TO TAKE APPROPRIATE ACTION.

ANDREW WOODS

TEAM OF THE YEAR

Woods was cited for his efforts with the Operations Analysis Group. In particular, "…he has established partnerships that integrate both service delivery and policy to better serve internal and external customers, and ensure stakeholders have access to resources necessary to take appropriate action. Woods most notably excelled in the process improvement category. His support from and responsibilities to each directorate to build and execute trend setting initiatives have strengthened DSS' mission effectiveness and efficiency."

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

Through the BRAC Program Management Office's efforts, the relocation of DSS Headquarters from Braddock Place to the new Russell-Knox Building was executed to near perfection.

The award also noted, "This alone was a herculean task; however, BRAC also coordinated and executed multiple office moves involving various DSS facilities, often simultaneously to include the relocation of DISCO from Columbus, Ohio, to Fort Meade, Md. The internal and external partnerships built and maintained by the BRAC team across the entire DSS enterprise were critical to the success of these efforts. This team exemplifies the level of superior performance that should be recognized and emulated."

RUSSELL-KNOX BUILDING:

The 2005 Base Realignment and Closure (BRAC) required the collocation of the "Military Department Investigative Agency (MDIA) Headquarters with the Defense Intelligence Agency and Defense Security Service at Marine Corps Base, Quantico, Va.," and to achieve full occupancy by Sept. 15, 2011. The co-location of these activities offers military leadership "world-wide situational awareness" under one roof.

As a result of the BRAC initiative, the Naval Facilities Engineering Command (NAVFAC) awarded a $312 million contract to the Hensel-Phelps Construction Company, headquartered in Greeley, Colo., to construct a new facility. In addition to the facility itself, the project included improvements to the site and construction of Tallmadge Road, which connects Russell Road to Telegraph Road.

The result, and new home of elements of the Defense Intelligence Agency, Headquarters of the Defense Security Service, Army Criminal Investigation Command, Naval Criminal Investigative Service and the Air Force Office of Special Investigations, is the Russell-Knox Building, a 718,000 square foot facility sitting on 100 acres.

While the past year has focused on the occupants of the building and the move of five disparate activities, the building itself has now received recognition from the Design-Build Institute of America (DBIA).

The building received the 2011 Regional Design Excellence Award and the 2011 Regional Design-Build Award, Office Buildings Category.

The DBIA Design Excellence Award honors projects that achieve an owner's overall aesthetic vision through outstanding design. The Russell-Knox design team was charged with designing a state of the art, stand-alone facility that complemented the "Georgian style"

DESIGNED FOR EXCELLENCE

architecture prevalent throughout Marine Corps Base Quantico, while at the same time respecting the individual identities of each of the five activities.

The award stated that the project's success in design demonstrated an exemplary commitment to achieving this mission and tremendous teamwork demonstrated by the five activities, NAVFAC, the architects, engineers, and construction firms to accomplish this task.

To be considered for a DBIA Regional Design-Build Award, projects must demonstrate successful application of design-build principles, including collaboration in the early stages of the project. The project must be completed on time, on budget and without litigation.

The Russell-Knox project involved accommodating the space and functional needs of five different activities, each with a distinct culture, work process, and specific space requirement that had to be incorporated into the design. These organizations emphasized security and respect for sensitive information.

Understanding each user group's needs involved management by the design team, which held concept design workshops with the agencies and NAVFAC, presented designs, and communicated throughout design and construction.

Established in 1993, and based in Washington, D.C., the DBIA is the only organization that defines, teaches and promotes best practices in design-build.

Design-build is an integrated approach that delivers design and construction services under one contract with a single point of responsibility. Owners select design-build to achieve best value while meeting schedule, cost and quality goals.

DSS COUNCIL SERVES EMPLOYEES

By Beth Alber
Public Affairs Office

The DSS Employee Advisory Council (EAC) first convened in May 2011 with the mission to provide DSS employees with an avenue to funnel recommendations and suggestions to senior leaders in support of the agency's mission, goals and objectives. It also facilitates the exchange of ideas between the various DSS offices, and serves as a clearinghouse for suggestions to enhance federal employee satisfaction and work effectiveness.

The EAC has its roots in a 2010 grassroots effort led by Preston Harper of Industrial Policy and Programs and a recognized need for improved communications across the agency. The original concept was for a venue that employees would feel comfortable using to share a comment, request a clarification or voice a concern.

The EAC evolved from this early concept and now includes a formal charter which outlines the composition of the EAC, determines how often it will meet and describes its goal to serve as a vehicle for coordinated assessment and evaluation of certain issues and objectives affecting DSS employees. Current EAC membership consists of 15 representatives from across the agency, to include representatives from all four regions of Industrial Security Field Operations.

As outlined in the EAC Charter, the EAC will be overseen by the DSS Chief of Staff or a designated representative. Drew Winneberger, Director of Industrial Policy and Programs, volunteered to take on the role. "I believed in the concept," Winneberger said, "and the potential value this mechanism would bring to the agency."

To ensure employees are aware of the existence of the EAC, the work it is doing, issues raised at the meetings and any actions taken, a web page was established on the DSS internal website. Within that page are links to the Charter, meeting minutes, and a list of EAC members.

Since its inception, the EAC has fielded a variety of topics to include telework/flexible work schedules, fitness and wellness, facility improvements, and transportation issues related to the recent BRAC moves. All queries are discussed at EAC meetings, and if the issue can't be resolved by EAC members, it is then forwarded to the office responsible for the action to garner a response.

All responses are reviewed by the DSS Director for awareness, with some eliciting a comment or clarification from the Director. The response is then forwarded to the EAC member who raised the issue, and it is then recorded in the EAC meeting minutes.

Some EAC topics have resulted in direct actions affecting DSS employees. After receiving numerous queries about the need for a physical fitness program, the EAC was the catalyst behind the policy developed by DSS Human Capital Management Office for a "Civilian Fitness and Wellness Program." The wellness program authorizes DSS employees

"I BELIEVED IN THE CONCEPT AND THE POTENTIAL VALUE THIS MECHANISM WOULD BRING TO THE AGENCY."

DREW WINNEBERGER, DIRECTOR OF INDUSTRIAL POLICY AND PROGRAMS

to take three hours of administrative time per week for fitness activities.

Recently, ensuring the anonymity of submissions to the EAC was questioned, so the Office of the Chief Information Officer proactively started the process for the creation of a web form, through which DSS employees can anonymously submit feedback, suggestions or questions to the EAC.

Other initiatives that are in progress include the creation of a matrix which outlines all DSS mandatory training and the timeframe it is due; posting notification letter templates and other operational-related letters to the web; and incorporating e-FCL training into Facility Security Officer training curriculum.

KEY DATES IN THE HISTORY OF DSS

1965: March 8, 1965, the Defense Industrial Security Clearance Office (DISCO) was established when more than 115 Army, Navy and Air Force clearance activities were merged

1972: Jan. 1, 1972, the Defense Investigative Service (DIS) was established to consolidate Department of Defense (DoD) personnel security investigations.

1980: Oct. 1, 1980, the Industrial Security Program, the Key Asset Protection Program, the Arms, Ammunition and Explosives Security Program and the Defense Industrial Security Institute were transferred to DIS from the Defense Logistics Agency.

1984: On Jan. 1, 1984, the Defense Industrial Security Institute in Richmond was redesignated as the Defense Security Institute.

1993: Jan. 6, 1993, Executive Order 12829 established the National Industrial Security Program (NISP) to replace not only the DISP, but also the industrial security programs of the Central Intelligence Agency, the Department of Energy and the Nuclear Regulatory Commission.

May 1993, DIS established a counterintelligence (CI) office.

1995: April 19, 1995, the Alfred P. Murrah Building in Oklahoma City was bombed killing 168 people, including DIS employees Bob Westberry, Larry Cottingham, Peter DeMaster, Jean Johnson and Larry Turner of the Oklahoma City Investigative Field Office.

1997: Nov. 25, 1997, DIS was redesignated as the Defense Security Service in order to reflect the agency's broader mission and functions, including the industrial security, personnel security, security education, and training missions.

1999: July 21, 1999, the Defense Security Service Academy was formally established.

2003: Feb. 4, 2003, the Commission of the Council on Occupational Education (COE), granted accreditation to the Defense Security Service Academy. The DSS Academy was reaccredited in 2009.

2005: Feb. 20, 2005, the personnel security investigations functions performed by DSS were transferred to the Office of Personnel Management.

2007: Dec. 18, 2007, the Director of DSS was named the functional manager for DoD Security Training.

2009: Jan. 15, 2009, the Deputy Secretary of Defense directed DSS to focus on meeting 21st century industrial security and counterintelligence needs by enhancing and expanding the NISP and reinvigorating the Security Training and Awareness Program.

DEFENSE SECURITY SERVICE