DSS ACCESS

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE

Volume 3, Issue 1

DSS HELPS TRAIN ACQUISITION PROFESSIONALS

SPRING 2014

Volume 3, 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 want to wish everyone a belated happy 2014. I know we're now several months into a new year, but this is our first ACCESS and a chance for me to recap 2013 and look ahead to 2014.

At the first senior staff meeting in January, I talked about the ups and downs of last year. My point in doing this was to emphasize that while it was a difficult year for the Defense Security Service, most of the challenges we faced in 2013 were beyond our control, most significantly the DoD-wide furloughs of last summer and government shutdown in October. What DSS could control, executing our mission, we continued to do and do well in spite of these challenges.

A highlight of 2013 was our success in transitioning the Command Cyber Readiness Inspections of cleared industry from the Defense Information Systems Agency. Since DSS became involved, we have been able to help industry prepare for these inspections while assisting industry in sustaining their system's hygiene.

We continue to make significant progress on automation initiatives that will move our oversight of cleared industry from a paper based process to an automated process. We are mapping requirements for a replacement to the Industrial Security Facilities Database that will not only automate many manual processes but will also facilitate collaboration across the agency. For more on our automation initiatives, please see the articles on the ODAA [Office of the Designated Approving Authority] Business Management System and DD Form 254 database. We also updated the Security Rating Matrix in September and released the ODAA Process Manual in November, which reflected a significant revision and consolidation of information into a format closely resembling information assurance instructions.

We achieved a number of milestones at the Center for Development of Security Excellence. We were the first DoD activity to obtain accreditation for the Security Fundamentals Professional Certification by National Commission for Certifying Agencies. Just prior to completing this issue, we received notice that the Security Asset Protection Professional Certification has also achieved the same national-level accreditation. We conducted a very successful beta test of the Industrial Security Oversight Certification and will be launching that program this year. We also introduced the Facility Security Officer (FSO) Toolkit, a one-stop shop of relevant information for FSOs.

These are just a few of our 2013 accomplishments; there are many more from across DSS. In looking ahead to 2014, I am optimistic and excited about the opportunities at DSS. Along with the rest of DoD, we will continue to manage a tight fiscal environment. But I believe DSS has made great strides in getting our fiscal house in order and we're well positioned to meet the challenges of the new year. We will continue to be the best at our mission and lead the industrial security community.

DSS HELPS TRAIN ACQUISITION PROFESSIONALS

By Stefanie Valero
Industrial Policy and Programs

DSS, through the Foreign Ownership, Control, or Influence (FOCI) Operations and International divisions, supports classes at the Defense Acquisition University (DAU) on a quarterly basis. The DAU provides a global learning environment to develop qualified acquisition, requirements, and contingency professionals at Government Contracting Activities (GCAs).

Our partnership with DAU bridges a gap between the acquisition and security worlds, supports synergies across DoD and other federal government agencies, and achieves collaborative results.

The two divisions from the Industrial Policy and Programs directorate, support the "DAU International Security and Technology Transfer/ Control Course", which educates GCA professionals on how to identify, analyze, and apply the laws, policies, and processes that govern international security and technology transfer/control.

In this collaborative training opportunity, International division personnel discuss a wide range of topics to include how they oversee and administer agency-level guidelines and international responsibilities regarding cleared U.S. industry involvement with foreign governments, foreign contractors, and the North Atlantic Treaty Organization (NATO) on behalf of the Designated Security Authority.

Presenters explain their development and support of transportation/hand carry plans, security violations involving foreign government classified information, processes for freight forwarders, foreign government visits to DSS, NATO sub-registry for cleared industry, international outgoing visit requests, foreign facility security clearance verifications, security assurances for cleared facilities and individuals and Limited Access Authorization requests.

Throughout the training, students are engaged directly with DSS subject matter experts in discussions on international security and technology transfer/control requirements and responsibilities. At the end of the course, students have DSS contact information to ensure ongoing collaboration and discussion.

Student feedback on the International section of the course has been positive with a common theme that indicates many students didn't realize the role DSS played in the International arena.

"We look forward to supporting this training," said Richard Stahl, chief of the International Division. "It's a great opportunity to provide information to the right people at the right time in the acquisition lifecycle and bridge the gap between the security and acquisition communities."

Presenters from the FOCI Operations Division share information on mitigating risks associated with FOCI under the National Industrial Security Program (NISP). These topics include how foreign acquisitions are reviewed and monitored in cleared industry and the various FOCI mitigation instruments available. One of the more complex mitigation instruments, the Special Security Agreement (SSA), covers classified information access limitations.

In order for companies to access the proscribed information (e.g., Top Secret, Sensitive Compartmented Information, etc.), the GCA must make a National Interest Determination (NID), which is a definitive statement that the release of proscribed information to the SSA company shall not harm the national security interests of the United States. Preparing the NID is the responsibility of the GCA, and this course provides students with direct training on how to properly prepare a NID.

Since FOCI Operations Division requests and tracks all pending NIDs for cleared industry, this course provides an opportunity for GCA personnel to directly share their concerns regarding NID requirements and responsibilities. As with the International course, the FOCI presenters provide contact information to facilitate future collaboration between DSS and the GCAs.

"This collaboration has been a learning opportunity for both organizations," said Ben Richardson, chief of the FOCI Operations division. "Our efforts at DAU have been part of a multi-level approach to educate the acquisition community on the requirements of the National Interest Determinations and the importance of timely processing to ensure that vulnerabilities are mitigated and contracts can be fulfilled."

Through this collaborative effort, the FOCI Operations and International divisions are contributing to the DSS vision of being the focal point of interaction and premier provider of industrial security and education services to the U.S. Government and the companies in the NISP.

FIELD OPERATIONS HOLDS

Leadership looks back

Senior leaders from the four regions and headquarters of Industrial Security Field Operations (IO) recently participated in a three-day leadership training workshop at Marine Corps Base Quantico, Va.

The agenda focused on four themes: Building a Conceptual Framework; Vetting Priorities; Framing Our Future; and, Evaluate and Execute. The training took these themes and applied them to the future operating environment, operational efficiency and effectiveness, resources and other management topics.

"Hosting managers from all regions and the headquarter locations is the best way to ensure a consistently high level of service and processes at every regional office," said Rick Lawhorn, Director, IO, in explaining the methodology behind the event.

He charged the IO leaders with helping craft the directorate future.

"Our success this year will be directly related to how we manage each challenge and how well we take care of our people. Providing opportunities like this to our leaders so they can provide the best care for our employees is a winning formula for everyone," he said.

As industrial security continues to be challenged by national and international incidents like the Edward Snowden classified information disclosure, Navy Yard shooting, and pending changes in intelligence oversight, the demands and expectations within DSS and specifically the IO Directorate become even more complex.

"This forum provided a tremendous opportunity for leaders to discuss and find hard-hitting solutions to very tough problems. Improving our ability and capacity to deter, detect, and mitigate security vulnerabilities is critically important to safeguarding our nations assets," said Lawhorn.

In his opening remarks, Stan Sims, DSS Director, said the large amount of positive culture change that has occurred in the agency in the past few years would not have been possible without the support of the IO leadership and the work of field personnel. "We were flexible, we managed the risk, and we continued to execute our mission," Sims said. "There is no one else who can do our mission."

Sims also emphasized the need for leadership to take care of the workforce while continuing to execute the mission. In

SENIOR LEADER TRAINING FORUM

and prepares for year ahead

summary, Sims praised the IO leadership for changing the DSS culture from an adversarial compliance methodology to a national security methodology.

Field Operations is the largest mission area in the agency with personnel located throughout the United States. Lawhorn noted that 2013 was a tough year due to budget constraints, furloughs and the government shutdown. "Despite these challenges, we did a lot of great work that we can continue to build on," he said.

Lawhorn highlighted several successes, to include the Command Cyber Readiness Inspection program, improved processes for annual meetings for companies operating under foreign ownership, control or influence, and updates to the Security Rating Matrix. "We need to get as much bang for the buck in this resource-constrained environment as we can," he said.

Lawhorn reminded the leadership team of the need to continually stress the work-life balance for staff in the field. He concluded his remarks by encouraging managers to say "thanks" to their staff for the work they continue to do and for keeping their eyes on the ball.

The IO senior leader group spent the first day and a half reviewing and refining IO's strategic objectives, establishing updated milestones and goals, and assigning ownership and tracking methodologies to ensure continuous movement towards improving oversight and support of cleared industry, and the preparation of the workforce for emerging missions and technologies.

Over the course of this three-day meeting, IO leadership met with representatives from many mission and support organizations to include Counterintelligence, Industrial Policy and Programs, Office of the Chief Information Officer, Human Capital Management Office, and Business Enterprise.

The intent of discussions with these entities was threefold: First, to maintain open lines of communication and information sharing across organizations; second, to gain an understanding of the many initiatives and technologies that are in the works for delivery in FY14, and third, to ensure IO's perspective and requirements are appropriately represented as new initiatives that are developed going forward. The leadership team met in February 2014 to continue building on the themes and processes introduced here.

CORPORATE SPLIT CHALLENGES DSS TEAM

> "I EXPECT OUR SECURITY TEAM TO CONTINUE TO BUILD ON THE GREAT PARTNERSHIP WITH DSS.

Stuart Shea, President and Chief Operating Officer of Leidos, Inc.

In September 2013, the Science Applications International Corporation (SAIC) officially split into two companies, with one part retaining the SAIC brand and the other becoming Leidos, Inc. Under the new companies, SAIC will solely focus on government IT services while Leidos will handle national security, commercial health and engineering sectors.

For DSS, this split resulted in a very complex review process to identify and then ensure that key management personnel, CAGE codes, accredited IT systems, etc., were appropriately aligned under SAIC or Leidos facilities. Approximately 85 cleared facilities and 22,000 cleared employees were affected. Personnel from DSS headquarters and field offices across the country all played a critical part.

For over 14 months, both companies worked with a DSS team, led by Justin Walsh, Chief, Facility Clearance Branch, to resolve any issues in order for Leidos and SAIC to operate as cleared defense contractors on the first day of the new organizations. "This split was unique for DSS primarily due to the size and scope of the effort," said Walsh. "Our goal from day one was to ensure that a smooth transition occurred resulting in uninterrupted mission support to the Government Contracting Activities that SAIC and Leidos support," Walsh added.

"We accomplished our goal and the success of this collaboration was truly a testament to the communication and partnership between DSS, Leidos, and SAIC."

To offer appreciation for the agency's support during the split, Stuart Shea, the first President and Chief Operating Officer of Leidos, visited DSS to meet with the team who worked the changes and present them with certificates of appreciation.

In his remarks, Shea said, "I consider the protection of national security information critical, not just for the success of our company but for the future of our country, and I expect our security team to continue to build on the great partnership with DSS."

Stuart Shea (right), President and Chief Operating Officer of Leidos, Inc., presents a certificate of appreciation to Justin Walsh, Chief, Facility Clearance Branch.

OBMS SCHEDULED FOR 2014 RELEASE

System will improve certification and accreditation process with automated workflow

The Office of the Designated Approving Authority Business Management System (OBMS) is set for deployment in fiscal year 2014, providing a key IT system to efficiently manage certification and accreditation (C&A) activities both now and into the future.

OBMS provides an automated workflow capability to support all aspects of the National Industrial Security Program (NISP) C&A process. The system is designed around a web-based portal that receives and stores system security plan (SSP) submissions from industry information systems security managers (ISSMs).

The system will also provide for automated tracking and notification throughout the system accreditation process. OBMS will replace the current e-mail submission and feedback process with a robust portal where ISSMs can submit, track, and update system documentation.

Access to OBMS will require DoD approved public key infrastructure (PKI) authentication at login, which is tightly coupled with the DSS NISP Common Access Information Security System. The system will not allow for user ID and password for authentication.

As a result, any potential users must have approved DoD PKI credentials by April 2014 to access the system. Approved credentials consist of government issued Common Access Card (CAC), External Certification Authority and DoD-approved Corporate Certificates authentication. Users will be required to complete the automated access request on the www.dss.mil website.

Once OBMS is launched, this enterprise application will significantly increase staff efficiency and productivity and improve reporting to provide capabilities for strategic risk planning of system assessments.

The Benefits and Features of OBMS Include:

- Web-based portal secured by DoD PKI authentication
- Central repository for SSPs and C&A records
- Real-time access to status information for accreditation packages while under review
- Automated notifications of SSP status changes
- Reporting features and capabilities to aid in monitoring the C&A process
- Interface for government stakeholders to submit supporting documentation
- Support for digital signatures on accreditation package documents
- Bulletin board forum for collaboration and knowledge sharing
- Method to capture National Industrial Security Program Operating Manual vulnerabilities
- Electronic Communication Plan metric tracking
- Centralized DSS authentication portal designed to lay the foundation for a single-logon capability for access to a number of DSS information systems (i.e. OBMS, ISFD, DD254)

WHAT IS A ... ?

>> DD FORM 254?

The DD Form 254, "Department of Defense Contract Security Classification Specification," conveys security requirements for the protection of information in the possession of cleared contractors associated with a classified contract.

A classified contract is any contract that requires, or will require, access to classified information (Confidential, Secret, or Top Secret) by the contractor or its employees in the performance of the contract. A contract may be a classified even though the contract document is not classified.

The use of the DD 254 alone cannot mandate requirements for the protection of information related to a classified contract. The requirement must first be established by the inclusion of the Federal Acquisition Regulation (FAR) Part 52.204-2, Security Requirements clause, included in contracts, grants, or other legal agreements between the Government Contracting Activity (GCA) and the cleared contractor. The security requirements can then be conveyed in the DD 254, as required by the FAR, and, as appropriate, in related Security Classification Guides.

The DD 254 is generally prepared by the GCA, but prime contractors are required to include a DD 254 in subcontracts requiring access to classified information. The DD 254 establishes the classification level and scope of access by the contractor. It normally includes information about the program and types of information to which the contractor will have access and is used by the contractor to establish its National Industrial Security Program (NISP) requirements.

DSS also uses the DD 254 to determine the scope of its oversight and assist in preparing for assessments. While the focus of the DD 254 is for the protection of classified information, the form provides space for supplementary guidance for the protection of other unclassified but sensitive material related to the classified contract.

In early February, the Under Secretary of Defense for Intelligence began an effort to revise the DD254 in conjunction with the process to replace the DoD Industrial Security Regulation. Another change for the form is automation. Though the DD 254 now only exists as a paper form, DSS is working to automate its use through the NISP Security Contract Classification System (NCCS). The NCCS will manage the DD 254 by providing a single, centralized, secure, web-based automated system for DoD and 26 other federal agencies.

Fielding NCCS is a priority for DSS, since there is currently no enterprise-wide system for managing the information required by the DD 254 and related contracts. NCCS will automate the capture of the data elements utilized to populate the DD 254.

>> LIMITED FACILITY CLEARANCE (FCL)?

By Lisa Gearhart
Industrial Policy and Programs

A limited facility clearance (FCL) is an option for a U.S. company under foreign ownership control or influence (FOCI) to access specific classified or technical program or contract information.

A Government Contracting Activity (GCA) or foreign government may sponsor a U.S. company for a Limited FCL. A limited FCL is considered when DSS determines that the U.S. company is under FOCI but the company is either unable or unwilling to implement FOCI negation or a mitigation agreement.

A limited FCL may be granted to foreign owned companies when: 1) There is an Industrial Security Agreement between the United States and the foreign government of the country from which the foreign ownership is derived; 2) release of the classified information is in conformity with established U.S. National Disclosure Policy; and 3) the FOCI is not negated or mitigated but simply accepted when a company is issued a limited FCL.

Access limitations to classified or technical information apply to all employees regardless of citizenship and only to the information that is specific to the program or contract.

A Limited FCL company may be a sub-contractor, but it is only for the program or contract specific information. In rare cases, the GCA may request a Limited FCL for a company based on a compelling need that serves critical national security interests, even when an Industrial Security Agreement does

The automation project is based in part on the adoption of functionality from the Department of Army's DD 254 system for its Sensitive Compartmented Information (SCI) contracts. Automated capture of the data elements is intended to address the lack of a central repository for DD 254 data, automate the DD 254 workflow from a paper/PDF driven process, allow for an accurate accounting of the classified contracts, provide assurance that the decision maker can access actionable data in a timely fashion, and better integrate the acquisition and the security communities.

NCCS will give leaders the ability to account for classified contracts under their authority and provide visibility that does not exist today into related sub and tiered contracts, supply chains, and technology related to contract information.

DSS is leveraging the functions from the Army system as the baseline Initial Operating Capability for the unclassified NCCS system. Once completed, NCCS will serve as a single source of record for managing all DD 254 contract-related information. Guidance on preparing DD Form 254 can be found at www.cdse.edu/documents/cdse/DD254.pdf.

not exist. The GCA's sponsorship request for a limited FCL should be signed by an authorized official of th e GC A an d sh ould in clude th e following statements: (1) The GCA understands that the FOCI will not be mitigated or negated; and (2) the GCA accepts the risks inherent in the granting of the FCL.

Subcontracting with a limited FCL company is not allowed for this scenario. Only the GCA responsible for the information in question can determine if release of the information is in conformance with National Disclosure Policy.

Issuing a limited FCL requires the concurrence of the DSS Office of General Counsel and FOCI Operations Division (FOD). The FOD will coordinate with the DSS Facility Clearance Branch throughout the limited clearance process to ensure the use of the limited FCL is in fact warranted and does not pose undue threat with regard to export control considerations. DSS will verify the limited FCL only to the specific GCA that requested it.

Credentialing Industry Leadership Award

By Nicole Graham
Office of Public and Legislative Affairs

In November, the Institute for Credentialing Excellence (ICE) awarded the Credentialing Industry Leadership Award to **Denise Humphrey** of the Center for Development of Security Excellence (CDSE). Humphrey received the award as the result of her innovative leadership in the field of credentialing and/or licensure by developing, implementing and researching programs or practices.

During the annual ICE Exchange, members of the international certification/credentialing community gather to present awards to its members. Humphrey is the first recipient from the Department of Defense (DoD) to have been honored with this award.

The forum acknowledged Humphrey's efforts as the chairperson of the Defense Security Training Council and Deputy Director of CDSE to lead the DoD-wide effort to design, develop, implement, and sustain a "private-label" certification program.

They further recognized the Security Fundamentals Professional Certification (SFPC) the first DoD professional certification to receive national level accreditation. SFPC is the first of the core certifications under the Security Professional Education Development (SPēD) program. During its development, Humphrey ensured the program addressed the needs of its stakeholders and ensure all involved in the program understood the needs, wants, and constraints of the program's various constituencies.

"I am humbled by being singled out, but this is truly a DoD Security Community achievement," stated Humphrey. "The DoD Security Community has blazed the trail for functional communities in developing certification programs and achieving national accreditation."

What is ICE? The Institute for Credentialing Excellence (ICE) community ranges from those who develop and enforce the standards for teacher licensure to groups who license and certify financial planners and anesthesiologists.

In order to be considered for the Credentialing Industry Leadership Award, an individual must be a current ICE member with a history of volunteer leadership or participation within the organization; work in the credentialing field at the time of nomination and at the time the award is presented; demonstrate significant evidence of contributions to the field of credentialing and; serve as an advocate to promote the benefits of credentialing to the public and/or the professional occupational communities.

After accepting nominations, the ICE Board of Directors determines awards the individual with the best demonstrated innovative leadership in the credentialing and/or licensure industry, as well as those who have demonstrated leadership in their service to ICE.

TWO NEW PLANS RECONCILE INDUSTRY

By Will Cooper
Industrial Policy and Programs

Competition, both local and global, has driven companies in the National Industrial Security Program (NISP) to take cost-reduction measures in bidding for federal contracts. Companies under Foreign Ownership, Control, or Influence (FOCI) are no different, and many FOCI companies find that sharing services and workspace with their affiliates reduces costs and increases competitiveness.

DSS, however, is obliged to mitigate all existing FOCI, including that which arises out of sharing costs with affiliates. To reconcile the agency's mission with industry's needs, DSS introduced two template plans that assist with FOCI mitigation while allowing companies to maintain their global competitiveness: the Affiliated Operations Plan (AOP) and Facility Location Plan (FLP).

AOPs: Theory and Practice

Affiliated operations are services and even personnel shared between a FOCI company and one or more of its corporate affiliates. These encompass everything from pension plans to legal counsel. For many years, companies would ask DSS's permission to share services one at a time, as there was no standard way of requesting, processing, or deciding on operations between cleared companies and affiliates. These inconsistencies led to confusion throughout industry about DSS's expectations, resulting in administrative delays and inadequate oversight.

DSS devised the AOP to address this confusion and empower the Government Security Committee (GSC) to take an active role in the FOCI company's relationship with its affiliates through a single, standard procedure.

While not all affiliated operations can be approved, a GSC can nevertheless help a company share resources with its affiliates by demonstrating to DSS that it can actively monitor and engage with those operations that can be approved. Seen in this light, the AOP is not a burden to industry but a tool for industry to streamline operations and lower costs.

As Benjamin Richardson, chief of the FOCI Operations Division (FOD), explained, "We want to help companies remain competitive in an environment where the FOCI is mitigated and controlled."

Since DSS released this template, the FOD has approved over 100 AOPs, demonstrating the plan is workable and acceptable to industry. Feedback from companies has been positive, and DSS encourages companies to provide their thoughts and suggestions regarding the template.

COST-SHARING WITH FOCI MITIGATION

As the defense industry becomes increasingly competitive, the FOD anticipates the number of AOPs will grow as companies increasingly look for cost saving measures for their business operations.

FLPs: Theory and Practice

Collocation occurs when a FOCI company's proximity to an affiliate inhibits its ability to comply with its FOCI mitigation agreement. In practice, this means that cleared facilities must maintain physical separation from their affiliates' office space.

Until recently, collocation was almost never allowed, meaning that FOCI companies could not share workspace even when convenient and cost-effective. This held true even where, for example, a FOCI company was located on the ground floor of an office building while its affiliate was located on the tenth floor.

DSS created the FLP in response to feedback from industry to allow collocation, with appropriate safeguards in place to mitigate FOCI arising from physical proximity.

Not all collocation can be approved, of course, but the FLP is another tool to empower companies to reduce costs by allowing for shared workspace under controlled circumstances.

While some companies misunderstand collocation, the FLP has been well received by industry, perhaps because it allows for a much less restrictive policy than had existed before. The policy helps DSS too, of course; as Richardson noted, "The FLP adds definition and a process to collocation where previously there had been none."

Collocations are assessed more consistently and uniformly now, and the process is more transparent to companies.

Plans from Partnership

If one juxtaposes the FLP and AOP, these seemingly separate agreements look rather similar: Both are templates crafted to reconcile industry's needs with the DSS mission, and both are corollaries to the more comprehensive FOCI mitigation agreements. Both plans allow companies to reduce costs while demonstrating to government stakeholders that classified information can be protected.

There is no question these collateral agreements will evolve in the coming months and years as DSS continues its dialogue with industry. By crafting these agreements for industry in response to industry, DSS adheres to Director Stan Sims' belief that the agency should form a partnership with industry. That dialogue, that partnership, continues apace.

SO YOU WANT TO BE AN FSO?

TOUGH JOB!

By Randy Stacey
Chantilly Field Office

While developing a presentation for a local security council, I searched for a good facility security officer (FSO) job description. While there were several job openings on the internet, all had very brief FSO duty descriptions and didn't work for the presentation.

So I decided to write my own.

Facility Security Officer:

Candidate must be able to deal with tight deadlines, complex situations, and ever changing circumstances. Will be required to deal with and answer to company senior management, program managers, employees, Government Contracting Agencies and government oversight agencies (i.e., DSS). Must be able to keep all the above happy and content throughout employment.

"Sounds like a tough job so far."

Person must be knowledgeable in personnel security, completion of personnel security questionnaires (SF 86), adverse information, and the reporting of adverse information. Must be proficient in the use of non-user friendly U.S. government database for the recording of security clearances, and able to use the Joint Personnel Adjudication System (JPAS) to submit or retrieve the above information, along with tracking clearances for scope and eligibility.

Must be able to track all personnel clearances, periodic reinvestigations, and special briefings (i.e. NATO, communications security (COMSEC)) requiring timely submission of updated information tracked by JPAS. Interpret and follow the instructions from JPAS Help Desk even though they may be vague or inaccurate.

"What in the world?"

Potential FSO must be knowledgeable in corporate/business structure to include foreign investors, legal entities, Key Management Personnel (KMP), corporate parent exclusion resolutions, and the mitigation of foreign ownership, control or influence (FOCI). Define which KMP clearances are tied to the facility clearance, and which may be excluded unless personnel clearances are needed to perform other duties outside of a corporate officer position.

Applicant should be able to correctly complete/submit U.S. government documentation to include Department of Defense Security Agreement 441, Appendage to Department of Defense Security Agreement 441-1, and Certificate Pertaining to Foreign Interest SF 328.

These duties include, but are not limited to, uploading all the previously stated information to an obscure U.S. government non-user friendly database known as "e-FCL" for review by a government agency with oversight responsibilities. The task will require multiple attempts and submission of said material.

"Now wait a minute, I didn't sign up for all of this!"

Candidate is expected to complete 13 (for non-possessing facility) or 18 (for possessing facility) government online courses as the FSO, plus an additional three courses annually to receive and maintain JPAS access.

FSO will be responsible for creating and providing initial and annual security briefings to all cleared employees. These briefings will include a threat awareness briefing and a defensive security briefing that will include an overview of the security classification system, which educates cleared employees on reporting obligations and requirements, security procedures and duties applicable to the employee's job.

"That's in the job description?"

Should employee fail to comply with the U.S. government regulations and/or guidance on the access and safeguarding of classified information outlined in the above training, the FSO shall submit a written report to DSS.

Should any information arise concerning actual, probable or possible espionage, sabotage, terrorism, cyber intrusion or subversive activities at any of its locations, said FSO is responsible for reporting this to the nearest field office of the FBI, copying their DSS office regarding information coming to the contractor's attention.

"Wow! That's a lot for one person to do. But wait there's more!"

Applicant will be an expert in safeguarding of classified material in the hands of industry to include but not limited to Confidential, Secret, and Top Secret information. Knowledge of how to store, courier, transmit, receipt, make disposition and destroy all of the above information in compliance with U.S. government regulations is required.

"How can one person be expected to do all of this?

Must be able to change combinations on GSA approved safes, design and negotiate construction of closed areas meeting government specifications, contract and procure intrusion detection system meeting UL 2050 specifications, obtaining and maintaining certification from third party evaluating institution, and verify and check the status of all classified material while in the possession of the cleared contractor facility. All applicants will also be expected to have knowledge of the Special Access Briefing which includes information about NATO, COMSEC, International Traffic in Arms Regulations (ITAR), immigration visa, international threats, Foreign Military Sales, foreign visitors and courier briefings,

"Forget it, I quit!"

The point in all of this is the FSO is responsible for an inordinate amount of information. They have the weight of several masters on their shoulders. They must be an expert in a wide array of information and disciplines. Most of all they must be a "patriot." They are our soldiers in the field working to safeguard this great nation.

Most do it out of the love they have for this country, not for the dollars they make. So remember that the next time you sit down for an assessment. Together DSS and industry are the active forces in the fight to protect the Warfighter and this great nation we call the United States of America.

*[**Editor's Note:** Randy Stacey presented this information at a recent Quantico Area Industrial Security Council.]*

A Q&A WITH **BARRY STERLING,**

Barry Sterling is currently the Chief Financial Officer and Director of Business Enterprise (BE) at DSS. He initially started with the agency on a detail from the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) in November 2006 as the Comptroller. He officially joined DSS in September 2007 as the Chief Financial Officer.

Sterling is a retired Air Force officer and spent his entire 23 year career in comptroller, cost analysis and budget. He held numerous positions from base budget officer, major command cost and budget officer, comptroller squadron commander and Director of Financial Management for Headquarters, Air Force Office of Special Investigations.

He retired in 2005 and worked as an Air Force civilian before moving to OUSD(I). During his time with DSS, Sterling has also been acting agency director and acting agency deputy director.

Business Enterprise encompasses several unique functions under one umbrella. What was your vision for BE when it was created?

About two years ago the concept of an integrated service function called 'Business Enterprise' came to fruition. We combined four main service elements — Financial Management, Logistics, Acquisitions, and the Chief Information Officer (CIO) — under one umbrella to create efficiencies and improve integrated service across the agency. Over the past two years, this concept has taken shape and developed into service support unlike any the agency has seen in the past.

By bringing these four functions under one umbrella DSS has unified the major resources of the agency: Formulating and executing the budget (Financial Management); rents and leases, property management, supplies and equipment, and vehicles (Logistics Management); Information Technology infrastructure and program development (CIO), and expenditure of funds through contracts (Acquisitions). All four of these functions must work as one.

How has this new organization helped achieve efficiencies and better integration at DSS?

Prior to the creation of BE, these four functions came under the operational control of different levels of senior leadership, which led to many disconnects.

For instance, DSS would go to open a new field office and logistics would lease and build out the space only to find the Acquisitions office had not purchased the furniture yet, or CIO had not laid cable or purchased the appropriate information technology equipment. As a result, DSS would end up paying rent on a new facility for months until the new space was ready. When it came time to relocate the office, a moving contract had not been put in place so further delays ensued.

Breaking through levels of operational control many times was difficult due to competing requirements. Disjointed planning and execution was the bane of the support elements existence.

Those dysfunctions have been eliminated now. We have combined review boards, with all four functional areas participating, that keeps leadership on the same sheet of music. We now have transparency and accountability where before there was none or very little. Projects are prioritized through the agency governance process, which now allows the CIO and other support functions to apply scarce government employees and dollar resources to the highest agency priorities. And expectations are managed through consolidated project lists with milestone progress oversight.

The next step we took in BE was to create one central location for submission of agency requirements. This meant that agency requirements could be tracked centrally and also gave us the ability to provide communications with the customer to help manage expectations.

In addition, standard furniture packages and standard IT equipment purchases allows us to better manage scarce resources and reduce waste. For instance, by standardizing printers, we moved to a few different models of toner cartridges vice dozens of different ones.

We have even automated the process with the Business Enterprise Services Toolbox (BEST). This portal will ensure DSS-wide situational awareness and will significantly strengthen collaboration. The BEST phase 1 (the first of three planned phases) was live in late 2013. Phase 2 will include process development, documentation and improvements and phase 3 will be the integration of all processes. The BEST phases 2 and 3 are planned for completion in the next 12 months.

The last piece added to the BE model was that of an Integration Office. This key critical position ensures that the internal service elements in BE are united to ensure requirements are managed in a consistent and coordinated fashion. This is achieved through advanced planning, collaboration, requirements clarification and communication. The integration office also serves as a liaison between the support functions and those that drive mission requirements. This has led to higher quality outcomes, allowing BE and DSS to deliver the right things, at the right time, in the right places.

Additionally the integration office plays a key role with external partners and agencies to help ensure projects and taskings are kept on track and placed in the DSS governance process to enhance organizational transparency. It also defines roles and responsibilities for key parties and constituencies and enables DSS leadership to make well informed, timely and integrated decisions that support execution of the overarching DSS Strategic Plan.

How has the budget environment affected BE and DSS?

Today's budget environment is one of the most difficult I have seen in my 31 years in the field. The budget uncertainty has presented agency leaders with difficult choices but also an unprecedented opportunity to fix broken processes, realign organizational structures, modernize technology, and make other improvements.

The BE model aligns perfectly with today's resource-constrained environment. The agency has gained efficiencies through better planning and execution leading to more effective use of resources. The improved use of integrated process teams has helped customers more clearly define requirements while the agency's governance structure has helped prioritize projects so scarce resources are applied most effectively to the highest agency needs.

What are the next steps for BE?

The BE concept will help the agency achieve audit readiness, particularly as it pertains to Property, Plant, and Equipment (PP&E). First, the four functional areas in BE developed a single shared vision of the PP&E environment and related processes. Next, audit readiness gaps and deficiencies were identified and corrective action plans were developed to mitigate those gaps.

This collaborative effort has resulted in effective physical inventories meeting audit standards, controls over recording asset acquisitions and effective controls over financial and management data in the accountable property system of record.

DSS ACHIEVES ACCOUNTABILITY

By Dewanda Marlow
Financial Management

The National Defense Authorization Act of FY10 mandated that the Department of Defense achieve fully auditable financial statements by Sept. 30, 2017.

The road to financial accountability was first established in the Chief Financial Officers Act of 1990, which laid a foundation for comprehensive reform of federal financial management and required auditable financial statements and strengthened accountability reporting.

To comply with the 2017 mandate, the Defense Security Service is one of the DoD agencies seeking to achieve auditable financial statements and in the process, has made great strides toward increased accountability and transparency.

As outlined in the FY10 NDAA, DoD produced Financial Improvement and Audit Readiness (FIAR) guidance that details the methodology and strategy for financial improvement and audit preparation. The FIAR Plan priorities were directed by the Under Secretary of Defense (Comptroller) and require DoD agencies to focus on improving processes, controls and systems.

The FIAR methodology includes a modified audit procedure that requires agencies to assess and test the design and operational effectiveness of its business processes and controls that impact the financial statements. This audit procedure also requires agencies to assess the sufficiency and accuracy of documentation used to support financial transactions that comprise various statements. These activities are summarized in a "management's assertion" letter presented to DoD asserting that the agency is "ready for audit."

Many believe the production and audit of private-sector style financial statements is superfluous primarily because the statements are not used to make financial and business decisions comparable to private industry.

The statements may not be used to make financial decisions; however at DSS, the process of achieving auditable financial statements resulted in increased employee accountability and financial credibility. In other words, the journey (achieving and maintaining auditable financial statements) may outweigh the destination (results produced by auditable financial statements).

One way the DSS audit effort has increased accountability is through categorization of data. In preparing for an audit or review, business activities and related transactions are categorized into assessable units, which are segments of similar business processes that together have a material effect on the financial statements. Property, Plant, and Equipment (PP&E) is one of those assessable units.

The culmination of financial data and activities required to achieve better controls and auditability over PP&E is presented on a federal version of a financial statement called the balance sheet. The balance sheet is often used in the private sector to provide investors insight on the strength and financial capabilities of a business. In DoD, this private sector analogy has limited use but understanding the process used to develop the balance sheet demonstrates its value and usefulness.

The process of achieving an auditable balance sheet requires, at a minimum, evidence through documentation of funding sources, to prove validity in the transactions and valuation of asset costs in accordance with strict accounting guidelines for accuracy. The federal balance sheet requires assets be segmented and accounted for differently than the more familiar programmatic or budgetary requirements. It also requires the automation and development of business processes that can be replicated through activities that drive reliable, timely, and competent financial information.

THROUGH AUDIT READINESS

At DSS, this effort resulted in an eight-month long process of locating the original funding documentation used to purchase assets. DSS, led by Business Enterprise, traced purchases and activities to funding sources, and then located, validated, and agreed to supporting documentation. As a result, the agency can attest to the costs, funding, and assets transferred to the receiving agency with a higher degree of confidence than estimates could.

The effort also required DSS to develop processes and controls to ensure information was readily available to employees to make business decisions.

In the past, the PP&E process didn't record certain assets in its balance sheet in a timely manner because the criteria needed for those decisions didn't reach the accountants until after the purchases were made.

Now, checklists, workflows, processes, and policies have been developed to provide financial guidance to nonfinancial employees creating an efficient paper trail for accountants and any external auditors (e.g., independent Public Accountants, DoD Inspector General, Government Accountability Office).

This accomplishment was due to collaboration and communication between Business Enterprise and the mission area directorates. DSS views its balance sheet as representative of the agency's improved ability to provide stewardship and accountability over assets and provide transparent, reliable and accurate information to senior leaders in making decisions.

DSS is also working to comply with former Secretary of Defense Leon Panetta's 2011 mandate of achieving an auditable Statement of Budgetary Resources (SBR) for General Funds in 2014. The SBR is a key financial statement that represents the status of all budgetary resources available to an agency in a given fiscal year. In June 2014, DSS plans to join several of its peers in asserting audit readiness to the SBR through accountability.

SPēD LAUNCHES MAINTENANCE AND

A major milestone for the Security Professional Education Development (SPēD) Certification Program was launched on Oct. 1, 2013: the Certification Maintenance and Renewal Program. Individuals conferred SPēD certification now have two years to keep their certification status in good standing.

Maintenance and Renewal Cycle

For individuals conferred between March 2011 and Sept. 30, 2013, the two-year maintenance cycle started Oct. 1, 2013, and ends Sept. 30, 2015. During this period, conferees have to exercise one of two recertification options: (1) Recertify by passing the assessment; or, (2) Recertify by attaining professional development units (PDUs).

For those conferred after Oct. 1, 2013, the recertification choices are the same but the maintenance cycle starts and ends on the conferral date. For example, for those conferred on Oct. 18, 2013, the maintenance cycle starts on that date and ends on Oct. 17, 2015.

"Conferred" means the Under Secretary for Defense for Intelligence (USD(I)) has signed and dated a certificate, and the conferral date is entered into the employee's STEPP records.

Recertification Requirements

Certification maintenance and renewal requires the accumulation of 100 PDUs within the two-year cycle. The PDUs can be attained by testing or through professional development activities. Individuals must be conferred one of the core certifications (Security Fundamentals Professional Certification, Security Asset Protection Professional Certification, or Security Program Integration Professional Certification) or specialty certifications (Physical Security Professional Certification or Industrial Security Oversight Professional Certification) to enter the Certification Maintenance and Renewal Program. There are six pre-defined categories in which PDUs can be earned.

1) Participation in Security Certification Programs

A community-recognized credential (i.e., certification) conferred to individuals who demonstrate mastery of a predefined set of knowledge and skills in a specified area. Certified security professionals will receive 100 PDUs for each SPēD certification gained during the defined two-year certification renewal cycle.

2) Participation in Non-Credit Bearing Training and/or Education Courses (or Certificate Programs):

An organized series of planned learning experiences (instructor-led or self-paced) developed and delivered to aid participants in acquiring specific knowledge, skills, and/or competencies associated with a topic area. Certified security professionals will receive three PDUs for each "contact" hour (or equivalent "seat time" hour) associated with an approved noncredit bearing training/education course or certificate program. There is a maximum of 45 PDUs for this category.

3) Participation in Credit-Bearing Training and/or Education Courses

An organized series of planned learning experiences (instructor-led or self-paced) designed and developed to aid participants to acquire knowledge, skills, and/or competencies associated with a coherent body of study within a discipline or set of related disciplines. Certified security professionals will receive 15 PDUs for each credit hour of an approved credit-bearing training/education course. There is a maximum of 45 PDUs for this category.

4) Participation in Conferences/Workshops

A conference is a live (in-person) or virtual meeting with presenters briefing participants on a wide range of interrelated issues/topics. A workshop is a working meeting or presentation with the goal of helping attendees develop knowledge or skills associated with a specific topic area. Certified security professionals will receive eight PDUs for each full day (or four PDUs for each half-day) of participation

RENEWAL PROGRAM

in an approved conference or workshop. There is a maximum of 40 PDUs for this category. Certified security professionals will receive an additional five PDUs for each presentation they give in an approved conference or workshop for a maximum of 25 PDUs.

5) Participation in Certification Projects

Certified security professionals may receive PDUs for successfully completing short-term certification projects (i.e., subject matter expert work on item development or certification preparatory tool or resource, participation in DoD Security Training Council working groups) that require application of security subject matter expertise. For each separate and distinct project the SME is involved in, 45 PDUs will be awarded.

6) Personal Experience and Achievements

Certified security professionals may receive PDUs for involvement in verifiable professional development experiences in security-related projects and activities. PDU values will vary depending on the activity.

It is the responsibility of each security professional, working with their supervisor or manager, to find the professional development activities that align with professional growth and/or organizational requirements, and to manage and track the professional development activities.

An online tool, the Certification Renewal Form, is available in "My SPēD Certification" to help personnel manage professional development activities and track the number of PDUs that have been submitted.

Professional development activities are not restricted to a single set found in a catalogue or from a single provider.

Taking stock of education and training activities across the DoD and federal government, there is a large selection available that will enhance professional growth and assist with maintaining an employee's technical expertise. A spreadsheet of courses, from numerous U.S. government organizations, is located on the SPēD Certification Maintenance web page: http://www.cdse.edu/certification/maintain-sped.html. This is a large list but it is not meant to be exhaustive.

Individuals are also encouraged to seek educational opportunities not only in security but in areas such as leadership development as there are many paths available to earn PDUs.

Get more information about the certification maintenance and renewal process at http://cdse.edu/certification/maintain-sped.html.

Rules Approved for Newest Security Certification

In December 2013, the Department of Defense Security Training Council (DSTC) approved the cut score and business rules for the newest DoD specialty security certification, the Industrial Security Oversight Professional Certification (ISOC). The business rules outline the requirements for those participating in the production release, including those for maintenance and renewal.

The ISOC is a specialty certification which measures candidates' knowledge on such competencies as information security, classification management, incident response, and physical security. It also focuses on competencies within the industrial security categories, e.g., the National Industrial Security Program Operating Manual, facility security surveys, and other industrial security-centric competencies. Security professionals conferred with the Security Fundamental Professional Certification (SFPC) may request to participate in the production version, which is expected for release in February 2014.

Over 300 candidates from across the DoD components participated in the successful ISOC beta test. Of those who took the test, 132 achieved a passing score. Of those who passed, 90 were DSS employees.

Through their participation, the assessment instrument was validated and the data collected enabled the DSTC to make an informed decision in setting the cut score. Candidates meeting the cut score have had their names forwarded to the Office of the Under Secretary of Defense for Intelligence for approval and conferral.

CDSE TRANSITIONING TO
INSTRUCTOR-FACILITATED ONLINE TRAINING

"I thought the instructors were great; they were available and knowledgeable. I liked that I could go at my own pace. I remember in the basic course that I was often waiting on my classmates to complete assignments, so it was nice to move on to the next thing when I was done instead of waiting around. I also liked that I was able to telework, and start and end my classroom work when it was convenient with my work caseload."

Testimonial from a student in the first DoD Advanced Personnel Security Adjudications Course offered in the instructor-facilitated online training format

Despite travel budget restrictions, security professionals have ample opportunity for quality training and education through instructor-facilitated online training courses.

The Center for Development of Security Excellence (CDSE) has successfully launched 17 college and graduate courses in this format. Courses are delivered using a collaborative online learning environment making them available to U.S. military members and government employees worldwide, and also providing students the flexibility to complete assignments at their own pace. Instructors engage students in online forum discussions, answer questions, grade assignments, and provide feedback.

CDSE is currently working on transitioning additional training courses to this format. This year, the instructor-led DoD Advanced Personnel Security Adjudications Course was redesigned into an instructor facilitated online course.

The newly revamped course incorporates presentations, practical exercises, and forum discussions. Using this format, students make final security eligibility determination decisions and prepare Statements of Reasons. This course is the first instructor-facilitated online training course offered by CDSE that is tailored for DoD national security adjudicators assigned to the DoD Central Adjudications Facility.

One of CDSE's most sought after courses, the DoD Security Specialist Course, is currently being transitioned to this new format. The DoD Security Specialist Course is targeted to entry-level DoD and federal agency civilian, military, and contractor security professionals.

The course is also suitable for information systems security managers, security administrators, program managers, declassification specialists, intelligence officers/analysts, and persons with additional duties as a security manager or who are seeking to enhance their knowledge of the security disciplines.

Office of the Registrar:
THE "HEARTBEAT" OF CDSE

The mission of the Center for Development of Security Excellence (CDSE) is to provide the Department of Defense with a security center of excellence for the professionalization of the security community and be the premier provider of security education and training for the DoD and industry under the National Industrial Security Program (NISP).

The Office of the Registrar administers and integrates the services provided by CDSE and Defense Security Service Academy. The office also has administrative oversight of the Security Training, Education and Professionalization Portal (STEPP), which is the gateway for students to access learning activities or courses and establish interest in the SPēD certification program.

The Registrar's office also provides a wide variety of student support services to the DoD security professional and industry partners in meeting their professional development needs.

Why is this office considered the "heartbeat" of CDSE? Because the Registrar's Office is the central structure within CDSE to which other program elements rely upon to successfully meet the mission.

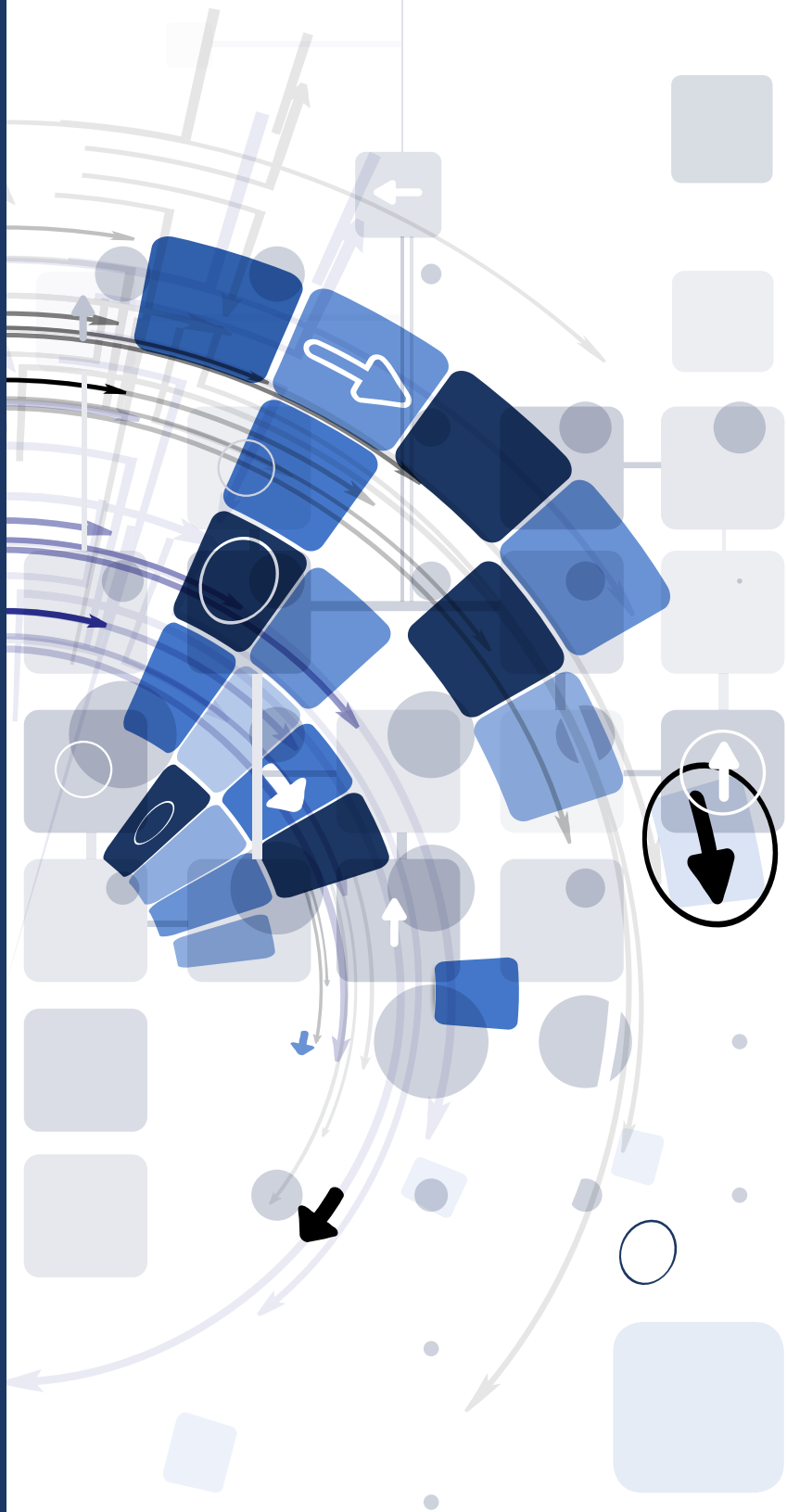
The office consists of a small team of customer-focused individuals driven to provide superior registration services. The members of the team are Kara Brown, team lead; Brittanny Yearwood, assistant registrar; and Harry Mitchell, assistant registrar, along with four other contractor personnel led by Rochelle Foster, registrar.

Each team member is dedicated to assisting and resolving education, training, and certification inquiries. More specifically, they provide support and assistance with:

- Providing solutions for telephonic and email inquiries
- Compiling statistical data
- Updating and printing official transcripts
- Managing and validating student records
- Maintaining the course catalog
- Maintaining the official system of records for the SPēD Certification Program

During fiscal year 2013, the Registrar's Office supported more than 285,000 active STEPP users and over 4,000 security professionals seeking certification. The office strives to meet customer needs as well as the organization's vision. High customer satisfaction ratings on customer surveys validated that office's high standard of service and distinction. The Office of the Registrar serves CDSE's goal of being the premier provider of security education, training, and certification services; they truly are the "heartbeat" of CDSE.

THE FOLKS BEHIND CASE STUDIES:



By John Massey
Operations Analysis Group

The Defense Security Service contributes to national security by serving as an interface between government and cleared industry. DSS administers and implements the defense portion of the National Industrial Security Program (NISP) pursuant to Executive Order 12829.

With this responsibility comes the need to ensure the timely flow of official information to agency personnel with a need to know. The Operations Analysis Group (OAG) acts as that catalyst in DSS, promoting the security of classified U.S. technologies and information in the hands of industry under the NISP.

Who We Are

The OAG was established in June 2010 and relies on a dedicated cadre of personnel comprised of subject-matter experts with diverse backgrounds in intelligence, security, and law enforcement to execute its mission.

OAG members are detailed from all four DSS mission directorates (Field Operations, Policy and Programs, Counterintelligence and the Center for Development of Security Excellence). The OAG also receives external support and participation from the Department of Defense Central Adjudications Facility (DoD CAF).

What We Do

The OAG serves as a conduit for information flow across DSS by facilitating information sharing while also conducting internal and external vulnerability gap analysis. The OAG reviews and identifies systemic and non-systemic vulnerabilities, that when taken in concert with threat and consequence, present an unacceptable risk to U.S. information and technology resident in cleared industry.

Since its inception, the OAG has reviewed more than 1,400 reports of information that meet one or more of the 18 reporting thresholds. As an example, the following thresholds have consistently been in the top three when looking at data on a quarterly basis over the last three years:

THE OPERATIONS ANALYSIS GROUP

1. Credible/relevant reports of potential espionage indicators exhibited by cleared personnel, such as unexplained affluence, keeping abnormal work hours, or seeking access to classified information without a need-to-know.

2. Notification of an investigation or arrest of cleared NISP personnel or the investigation of a NISP facility.

3. The unauthorized penetration or disruption of information systems containing classified information or information critical to national security, when the involvement of a foreign power or terrorist group or individuals acting on their behalf cannot be ruled out.

All DSS elements are educated on OAG reporting thresholds through internal guidance, information products, and web-training. These thresholds are reviewed and updated on a periodic basis. The reports originate from a variety of sources to include the DSS directorates, field personnel, the DoD CAF, and other government agencies. The OAG also relies on open-source media reports involving NISP companies and employees for additional information. Two-thirds of all reports elevated to the OAG originate from the industrial security specialists or field counterintelligence specialists in the field.

Mitigating the Vulnerability

The OAG follows a triage process that consists of analysis and review to identify vulnerabilities associated with each case. On average, 80 percent of the cases the OAG reviews uncover an existing and unmitigated vulnerability. These vulnerabilities can be internal to DSS and/or the U.S. government, external to industry, or both.

The vulnerabilities are further defined as non-systemic or systemic in nature. Systemic vulnerabilities are generally associated with policy, process, technology and execution issues. Mitigating and resolving these vulnerabilities is accomplished either by updating or clarifying existing policy, recommending new policy, reviewing current processes, and/or providing additional training.

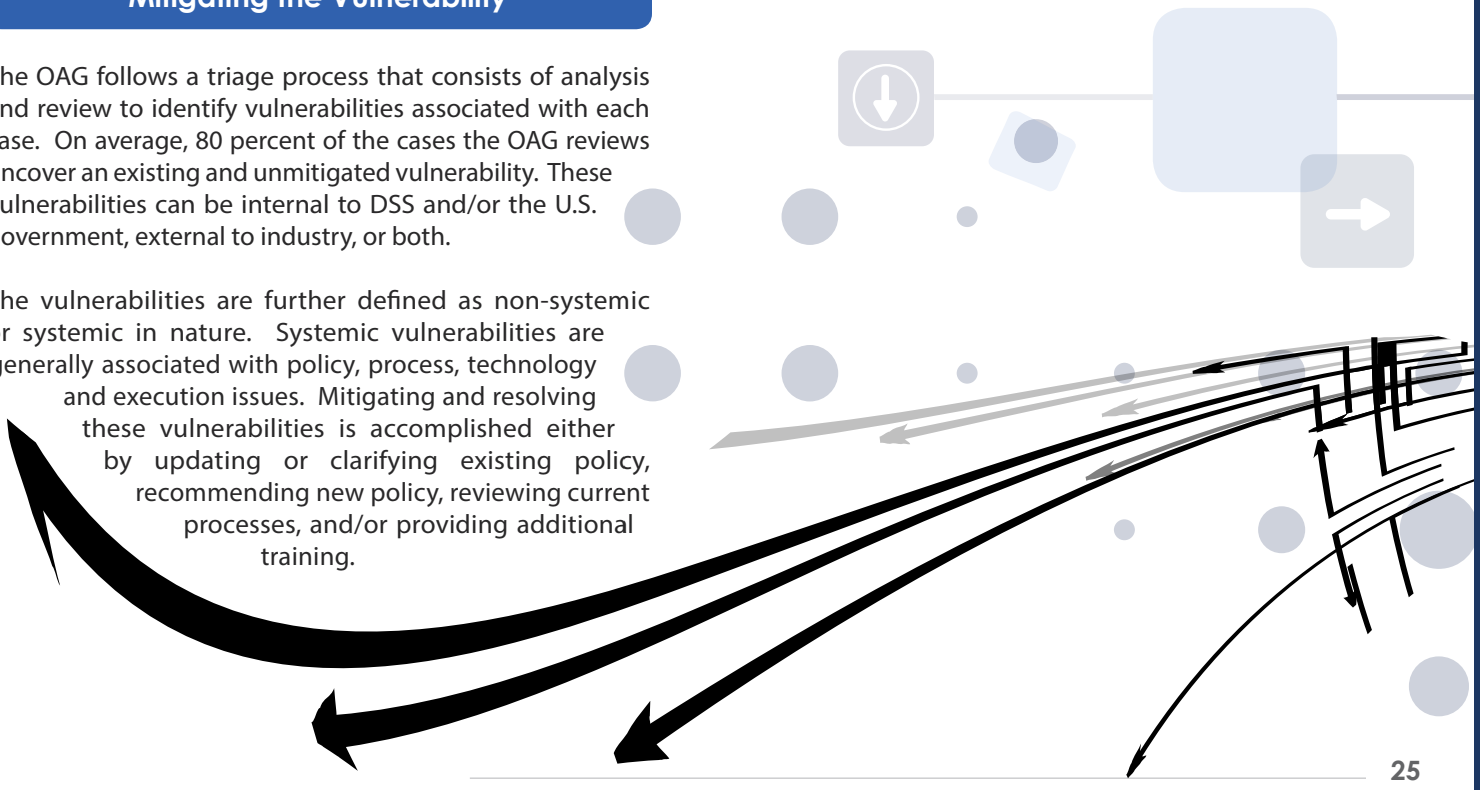
Non-systemic vulnerabilities are primarily isolated incidents that are difficult to preclude but nonetheless require mitigation and immediate action upon detection. To date, over 1,000 vulnerabilities presenting unacceptable risk have been mitigated as a result of OAG actions and recommendations.

Case Studies and Feedback

In addition to vulnerability mitigation, the OAG provides feedback to DSS directorates and field personnel on a variety of issues and trends and elevates matters of significance to DSS senior leadership. The OAG also provides feedback to industry in the form of case studies. These case studies are produced as a service to the DSS workforce, cleared industry, and the security and intelligence communities.

Case studies are unique and focus on the discovery and identification of vulnerabilities and mitigation action taken following OAG review. The case studies also provide lessons learned, best practices discovered, and training that may be available to prevent future vulnerabilities.

Case studies are featured in each issue of the DSS ACCESS. Case studies releasable to industry are available by contacting your local DSS industrial security specialist.



TRANSFORMATIVE MILITARY TECHNOLOGIES: First in a Series

THE STIRRUP

The "next big thing" in technology may not be big at all but instead, a small change to current equipment.

DSS works to protect the classified information and technology resident in U.S. cleared industry. Many times the focus is on protecting major programs, such as the Joint Strike Fighter, missile technology, or satellite electronics.

There are examples throughout history where the successful protection of a major new technology has had a significant impact on the outcome of a conflict; the use of radar by the British in World War II is a perfect example. But the protection should extend to even small advances that at first glance might not seem as important. Sometimes only a slight modification to an existing technology or a combination of small changes can have also have a big impact.

The stirrup is a humble thing: a resting place for a rider's foot that attaches to either side of a saddle. This simple device is a standard part of most saddles today, so common that many riders probably take it for granted.

The addition of paired stirrups to the saddle — not just for mounting, but as an aid to rider stability and control — originated in China sometime between the third and fifth centuries AD. This modification to the saddle came to Western Europe during the Middle Ages — coinciding with the rise of the mounted, armored knight. Thus, to this simple technological modification can be attributed the transformation of society by ushering in feudalism.

The Beginning of Feudalism

Feudalism, at its most basic level, was a political system based on land grants in return for service. The lord granted land to the vassal in return for an oath of fealty, a pledge of loyalty and support to the lord. This basic relationship applied to the nobleman or knight who received large manors from the king, on down to the serf who received a small parcel of land from the local lord for farming.

The more land that was granted, the bigger the obligation. A serf might be required only to provide a portion of his crop to the local lord, plus a few days of service, whereas a nobleman or knight could be required to provide military as well as financial support to the kingdom.

Lynn White, in his book *Medieval Technology and Social Change*, had perhaps the most famous connection between the stirrup and the rise of the feudal system. White argued that the rise of cavalry in western Europe, and by extension feudalism, began with Charles Martel and the Franks in the early eighth century.

In 718, Charles Martel rose to power as the ruler of Francia. He spent much of his reign fighting to stop the Moorish advance into Europe. Around 732, Martel also began confiscating large amounts of church land. The church was very powerful at the time, so confiscating its lands could have serious political consequences. At about the same time (based on archeological evidence), the military use of armor, heavy saddles, and lances increased.

Facing the persistent threat of invasion, Martel saw the value in having a professional fighting force. Although he defeated the

The humble stirrup

Moors, he saw the devastating impact of their mounted soldiers. He used the confiscated church land to establish horse farms for the knights who would become his professional soldiers. As more knights were granted land in payment for services rendered and for their pledge of fealty, the system of feudalism gradually spread across Europe.

The Impact of the Stirrup

The stirrup, on its own, is simply a useful device. But its impact on European society was profound as it contributed to the rise of the mounted knights, making cavalry the dominant fighting component in warfare for centuries.

The stirrup provided a stable fighting platform from which the knight could fight in battle. It allowed a knight, weighed down with 40-60 pounds of armor, to more easily keep his balance in the saddle against the potential upsets of combat.

Because the stirrup made it easier for riders to remain mounted during battle, the level of riding skill required was reduced, which allowed for more knights. More knights meant more land grants in payment for their services, and a greater number of trained warriors available to protect the kingdom.

The "next big thing" in technology may not be big at all, but instead, a small change to current technology or equipment, like adding stirrups to a saddle. To maintain the nation's technological edge, DSS will continue its mission of protecting all classified technical advances, big and small.

COUNTERINTELLIGENCE DIRECTORATE ACTIVELY SUPPORTS OPERATION WARFIGHTER

In their own words:

Cardoso notes, "I didn't know what to expect upon arrival at the civilian facility; but the staff was very friendly and any questions I had were answered immediately. The job is exciting, and I have learned what it takes to conduct civilian work and what it takes to be successful in the civilian world after my military career is finished."

Army Staff Sgt. Jose Cardoso (a Purple Heart recipient) began his internship at the CI Field Operations Division, Western Region (Tacoma, Wash.) in October 2013 under the supervision of Ray DuVall, FCIS, and Darrin Slovanick, Field Office Chief.

The Defense Security Service has participated in the Operation Warfighter (OWF) program since 2011, and the Counterintelligence (CI) Directorate has been an active participant from its inception.

To date, the CI Directorate has worked with seven recovering service members, all assigned to the field (five in the Western Region and two in the Southern Region). These service members represent enlisted and officer, National Guard, Reserve and active duty military.

Although the OWF program is a wellness program for service members who are recuperating from their injuries, these men and women view internships with DSS as another way to continue serving their country.

Each OWF participant has assisted field counterintelligence specialists (FCIS) in identifying penetrators of the Defense Industrial Base by conducting open and classified research, preparing security vulnerability assessments support packages, drafting suspicious contact reports, answering ad hoc requests for information in support of the agency's CI and security missions, and performing other duties as assigned by the supported FCIS.

The DSS Human Capital Management Office (HCMO) works closely with CI and other participating directorates to ensure a successful OWF program. Management support of the program is key, notes Leila De'Vore, OWF program manager in HCMO.

"OWF is such an important program and CI's support has been phenomenal," she said. "They provide wounded service members with the motivation to move forward and positively impact them in a supporting work environment.

"For CI, providing OWF internships is an easy decision," De'Vore continued. "While these internships give federal employees the chance to help wounded service members transition from military to civilian life, it also gives the wounded service members an opportunity to continue supporting their brethren in a different capacity. I'm pleased to work with such a passionate team!"

De'Vore frequently coordinates with Tom Montero, chief of CI Operations, Western Region and Jeff Boick, acting deputy chief of CI Operations, Western Region, on OWF opportunities.

Montero is committed to ensuring OWF internship opportunities are available to service members: "Our concept of support to the Wounded Warriors is, first and foremost, to provide them with the skills they can use in transitioning to a job in the civilian world, with another federal agency, or within DSS itself.

"In addition to providing training in all aspects of counterintelligence analysis, an introduction to the National Industrial Security Program (NISP) and improving their written and verbal communications skills, we also review and provide feedback on their resumes and offer guidance on how to interview for a job," Montero added.

Montero and Boick often represent DSS at Hiring Heroes career fairs, events at Camp Pendleton, and Family Day at Balboa Naval Hospital in San Diego. "Engaging these Wounded Warriors leaves us emotionally drained, but highly satisfied that we are taking care of one of our own," said Boick.

According to De'Vore, the DSS goal is to increase the number of OWF internships from 25 in fiscal year 2013 to 49 in fiscal year 2014. To date, two service members have been placed in OWF internships this fiscal year. The length of OWF internships varies depending on the service member's rehabilitation process, and work performed is arranged between supervisors and a participant's warrior transition unit.

Marine Corps Reserve veteran Staff Sgt. Sergio Esquivel participated in the DSS OWF program from June through November 2012 at the CI Field Operations Division, Western Region (San Diego, Calif.) under the supervision of Tom Montero.

During his internship, Esquivel used the information he obtained through his master's degree in Computer Information Systems, in conducting analysis on cyber-related suspicious contact reports. His tenure with DSS helped him get a job with a government contractor on Camp Pendleton.

Esquivel describes his experience in the DSS OWF program:

"It was great to get real-world experience in the field of counterintelligence and work with Mr. Montero and his team. I was able to use many of the skills I had picked up in my time as a Marine, in combat and in the fleet, and also through school, to assist the FCIS's efforts to fulfill their mission. It was a blessing to go home every day knowing the work I was participating in was helping to keep America's technologies safe," Esquivel said.

"Overall, it was an honor and pleasure working with Mr. Montero and his team. They were not only highly experienced in their field but had a genuine passion for the work they did. This proved to be the biggest takeaway from the experience," he continued. "Although I was not able to stay with DSS for as long as I would have liked, because of this experience, I will always strive to find a career that I can be passionate about, surrounded by like-minded people, until the day I retire."

Field Office, NCMS Join Forces to Sponsor FSO Training Event

By Gary S. Layne
Virginia Beach Field Office, Industrial Security Field Operations

After hearing constant feedback from facility security officers (FSOs) with comments like: "I love coming to the local NCMS meetings, but I wish they would provide training for new FSOs or for additional duty FSOs," former local NCMS Chairman Tameka Watts, FSO for SAIC, decided to act. She approached me with the idea of holding a two-day training session for FSOs.

After some planning discussions, the Virginia Beach Field Office agreed and decided the target audience would be FSOs with two or fewer years experience and those that hold the position as a part-time collateral duty. In September 2013, approximately 134 FSOs participated in local FSO training presented by experienced FSOs, Cogswell winners, and DSS professionals, held at the Lockheed Martin Center for Innovation, Suffolk, Va.

The purpose of the training was not to engage in areas of more complexity but rather to assist the new FSOs with advice, knowledge, and confidence that the FSO position is manageable as long as you complete your FSO courses, work with your local DSS representative, and build relationships with other professionals in the industrial security arena.

The agenda covered 13 major industrial security topics, used interactive games designed to highlight specific security areas, and featured a DSS panel that provided answers, guidance, and suggestions on how to improve the security posture of the participants' industrial security programs.

Now, we're hearing feedback like the following from FSOs:

Annamarie Kay, Antech Systems, Inc.: "First, let me say how much I enjoyed and learned (again) from the new FSO training. It was a great and valuable event. I know the new FSOs that sat around me at the conference really learned a lot. Hopefully, we can have this become an annual event."

Joe Varbero, TST Tactical Defense Solutions: "A key component of the event highlighted the fact that we are all working together to safeguard the same thing regardless of the government/industry/competitor relationships. I took away a better idea for securing information through processes that are approved by DSS and not burdensome to the companies. The training further developed my network of trusted professionals in this arena."

Lori Lorenz, Whitney, Bradley & Brown, Inc.: "I thought the new FSO training was a very helpful way to introduce the new FSO to the procedures which are most often part of the FSO's day. It also provided a great avenue in order to ask questions and provide resources, as well as network with others. We are all in this together after all!"

Regional Visits by Leadership

By Nicole Graham
Office of Public and Legislative Affairs

During December, DSS leaders traveled to three of the agency's four regions to meet with employees, share successes from 2013 and look ahead to the new year. Visiting field offices and engaging directly with employees across DSS has been a priority for Director Stan Sims since he arrived.

These visits came at the end of a stressful, challenging year for the agency and employees. At each stop, Sims met directly with employees to hear their concerns and shared his vision and priorities for 2014.

In early December, Sims visited the Western Region and San Diego Field Offices where he received a briefing on current operations, took a tour of the offices, and met with personnel. He also attended a briefing and toured the production area at Northrop Grumman Systems Corporation in San Diego. When speaking to Northrop Grumman and DSS attendees, Sims remarked on the need for a continued partnership with industry in order to secure our national assets.

From there, Sims visited the Southern Region and Irving Field Offices, where he participated in discussions led by regional senior leaders on the status of the Southern Region and the future vision for DSS. The

DoD Recognizes DSS' Employment of Individuals with Disabilities

By Carolyn Lyle
DSS Equal Employment Opportunity Office

In observance of National Disability Employment Awareness Month, the Department of Defense (DoD) presents awards to DoD components for outstanding achievements in employment of individuals with disabilities.

The Defense Security Service (DSS) was selected as the Best Small Component for Achievements in Employment of Individuals with Disabilities out of a total of 25 small DoD components.

Components were ranked in eight categories, and DSS achieved the highest ranking in the participation rate of individuals with targeted disabilities in the workforce as of March 31, 2013, and for the increase in this participation rate since 2012.

Additionally, DSS achieved the second-highest ranking in the hire rate of persons who claim veteran status with 30 percent or more disability. As compared to the rest of the field of small components, DSS achieved the highest combined score in all eight categories.

The DSS Equal Employment Opportunity Office (EEO) worked with the DoD Office of Diversity Management and Equal Opportunity on a Workforce Recruitment Program (WRP) and the development of a DoD mentoring program for people with disabilities. DSS EEO created an internal pilot program where eight managers mentored and participated in counseling and coaching of eight WRP students with disabilities and engaged them for future employment with DoD.

DSS EEO worked with the DSS Human Capital Management Office (HCMO) to develop a hiring initiative for people with targeted disabilities, which asked each DSS directorate to allot one of its current open positions to be filled by an individual with a disability.

DSS EEO also had a WRP intern who assisted in the outreach and communication of the disability program to schools and vocational rehabilitation centers across the country to create outreach and marketing opportunities for the agency, in an effort to meet the DoD goal of two percent representation of persons with targeted disability in the employee population.

The combined efforts of the DSS EEO Disability Program and the DSS HCMO Recruitment Office, as well as senior management support, resulted in these achievements in employment for persons with disabilities.

The momentum will continue for fiscal year 2014 as DSS has demonstrated its commitment to the highest achievement in employment for persons with disabilities.

Highlight Successes and Challenges

event concluded with a visit to Lockheed Martin Aeronautics Corporation in Fort Worth, Texas.

Closer to home, Sims and Deputy Director Jim Kren visited the Capital Region and Alexandria, Va., field offices to hear a presentation on current operations, take a tour of the offices and meet with personnel. Sims also used the opportunity to present a number of awards and retirement certificates to employees.

In his remarks to employees, Sims recognized that the hard work of DSS personnel, in a rapidly changing security environment, has helped to improve national security. He challenged industrial security representatives to become "masters of their craft" and ensure they were practicing quality over quantity when conducting assessments. Sims said he was pleased to congratulate the field offices on their success in developing a better partnership with industry and stated that DSS enjoys a reputation with industry like no other time in the agency's history.

Sims acknowledged that this has been a difficult year for DSS employees and shared his priorities for 2014. He stated that retaining all DSS personnel will be his top priority and will ensure the DSS workforce has the technological resources needed to efficiently and effectively complete its mission. In order to diminish the burden of excess paperwork, DSS will work to increase research and development efforts to move away from antiquated systems. At each session, Sims thanked DSS employees and urged them to continue telling the good news DSS story.


DEFENSE SECURITY SERVICE