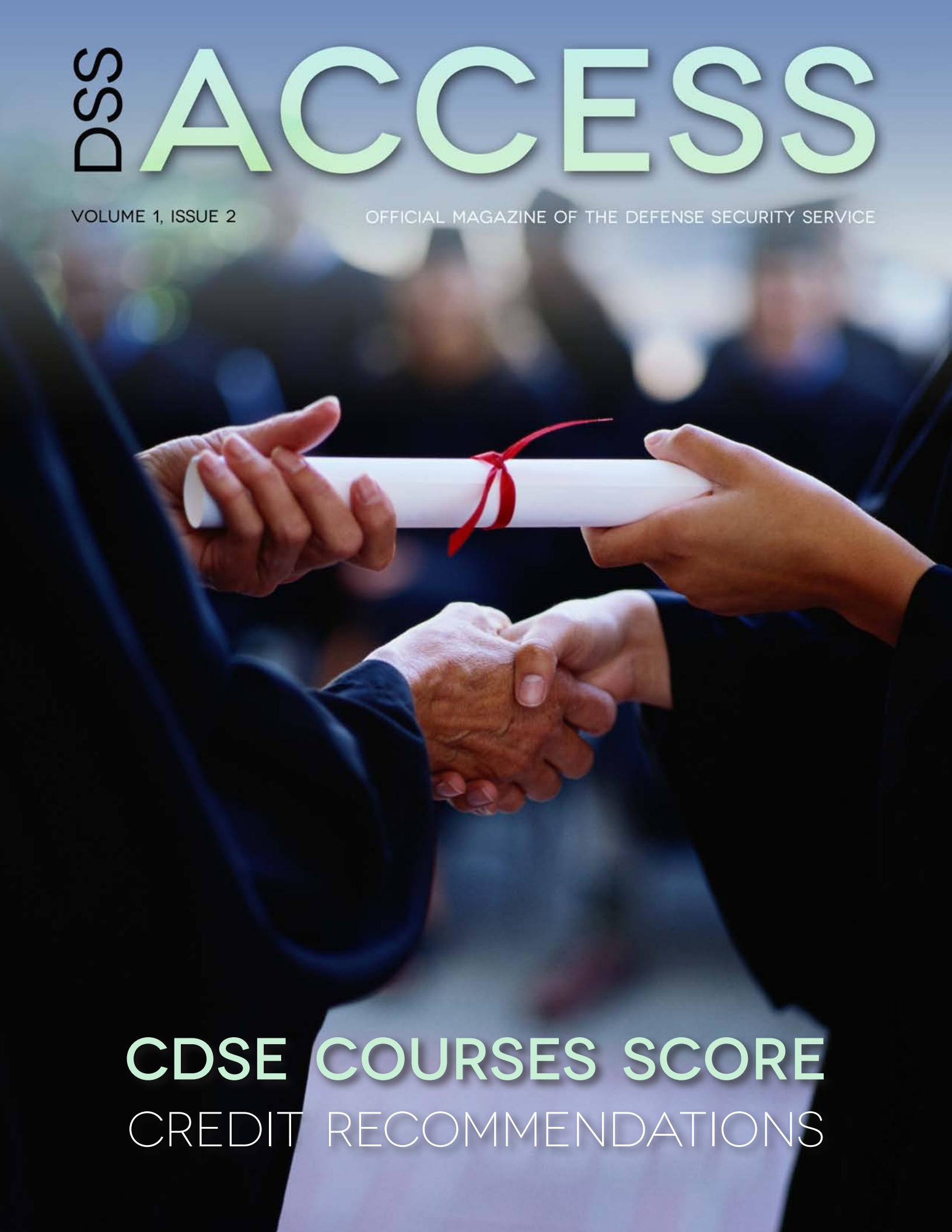
DSS ACCESS

VOLUME 1, ISSUE 2

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE



CDSE COURSES SCORE CREDIT RECOMMENDATIONS

SUMMER 2012

VOLUME 1, ISSUE 2

SPOTLIGHT

INSIDE

COMING TOGETHER

COMMEMORATING THE VICTIMS

DSS CASE STUDY

BEFORE AND AFTER

AROUND THE REGION

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

The launch of our new magazine was a tremendous success! I have received nothing but favorable comments on the first issue of DSS ACCESS. We set a high bar with our inaugural issue, but it's one I'm confident we will continue to meet.

I want this publication to continue to inform our industry and government customers about DSS initiatives, policies and procedures. I also want to provide a peek under the tent, if you will, to give you insight into our personnel, how they do their jobs, and how they are making a difference — not only at DSS but also in their communities. This second issue does just that.

This issue has several articles from the Center for Development of Security Excellence (CDSE). Of particular note is the cover article, which highlights the four courses CDSE offers that have been evaluated by the American Council on Education's College Credit Recommendation Service and recommended for college credit. This is not only a significant milestone — and opportunity — for DSS, but for every student enrolled in these courses.

We've included two case studies in this issue — one from our Operations Analysis Group (OAG) and another from the Boston Field Office. The OAG continues to look across the agency to improve our internal processes and reporting to ensure we are taking appropriate, timely and relevant action with regard to our oversight mission. And from Boston, we learn firsthand how DSS field personnel worked with a cleared facility over a two-year time period to help them move from an unsatisfactory security posture, to a superior rating.

We've also included articles on our International Branch, DSS support to a new NCMS chapter, as well as a roundup of actions from around our Regions.

Finally, we recognize the 17th anniversary of the Oklahoma City bombing and the five DSS employees who perished that day. For the first time, we had a representative, our new Chief of Staff, attend the annual memorial ceremony and meet with family members.

I continue to be impressed by the outstanding work done by DSS employees on a daily basis and I am excited to share their stories with you.

CDSE COURSES SCORE CREDIT RECOMMENDATIONS

Four courses offered by the Center for Development of Security Excellence (CDSE) have been evaluated by the American Council on Education's College Credit Recommendation Service (ACE CREDIT) and recommended for college credit. The courses are:

- Facility Security Officer (FSO) Orientation for Non-Possessing Facilities
- Facility Security Officer (FSO) Program Management for Possessing Facilities
- Introduction to Special Access Programs (SAP)
- Special Access Programs (SAP) Mid-Level Security Management

These courses were selected by CDSE as the first to be considered for college credit recommendations as they were amongst the most popular CDSE courses and readily transferable to document information required for the ACE review.

According to Brian Miller, chief of the Training Division, "The SAP courses are two of our longest running and most well-established courses," Miller said. "The FSO courses serve thousands of students making it one of the most popular curricula offerings. We picked the courses and the curricula so we could get the biggest bang for the buck and to ensure we were addressing both our government and industry student communities."

Miller explained the process students follow to "convert" the CDSE courses with credit recommendations to college credit. Each student who completes one of these courses will receive a certificate of completion from CDSE that includes the credit recommendation. If a student is enrolled in a program of study at a college or university, and they would like the institution to accept transfer of the credit recommendation, they must submit the request directly to that institution. The college has the option of accepting the ACE recommendation as a transfer and granting the equivalent college credits. "We're not involved in the process," added Miller, "it's the student's responsibility to follow through."

> "WE PICKED THE COURSES AND THE CURRICULA ... TO ENSURE WE WERE ADDRESSING BOTH OUR GOVERNMENT AND INDUSTRY STUDENT COMMUNITIES."
>
> BRIAN MILLER,
> CHIEF, CDSE TRAINING DIVISION

ACE recommendations for college credits are just that, recommendations, but Miller estimated 60 percent of the colleges and universities in the United States adhere to ACE standards. "The credits don't have value until the college or university accepts them," he said.

The FSO curricula (Possessing and Non-Possessing), and the Introduction to SAP courses all achieved a recommendation for two semester hours in the lower division baccalaureate/associate degree category. That equates to a freshman/sophomore, or 100/200 level course. The SAP Mid-Level course achieved a recommendation of two semester hours in the upper division baccalaureate/associate degree category — a junior/senior or 300/400 level course.

Dr. Ruth Grimes-Crump, director for Academic Assurance and Compliance at CDSE, explained the process for

ABOUT THE AMERICAN COUNCIL ON EDUCATION:

The American Council on Education, the major coordinating body for all the nation's higher education institutions, seeks to provide leadership and a unifying voice on key higher education issues and to influence public policy through advocacy, research and program initiatives. ACE CREDIT connects workplace learning with colleges and universities by helping adults gain access to academic credit at colleges and universities for formal courses and examinations taken in the workplace or other settings outside traditional higher education.

For more than 30 years, colleges and universities have trusted ACE CREDIT to provide reliable course equivalency information to facilitate their decisions to award academic credit. For more information, visit the ACE CREDIT website at *www.acenet.edu/credit*.

achieving an ACE recommendation. "ACE looks at every aspect of the course," she said. "There are 12 different standards that must be met. For instance, documentation must be presented relating to how the course content is presented, how we assess student knowledge, the course prerequisites, and course rigor and complexity."

Both FSO curricula are in fact a compilation of 13 to 17 individual courses. According to Grimes-Crump, CDSE "bundled" the curriculum to obtain the ACE credit recommendations. "Some of the individual courses are one to two-hour courses that would not qualify for college credit," she said. "But when we put them together as part of a larger program or complete curriculum, they do."

Grimes-Crump said the ACE action was a major milestone for CDSE. "This step gives our institution additional credibility, and demonstrates that our courses are of high quality," she said. "Our end goal is to have every course we provide have some credit value that is recognized and considered for transfer outside of DSS."

CDSE has taken a number of steps to announce the change and ensure students are aware of the opportunity for college credits. CDSE now appears in the National Guide, which is a listing of organizations for which ACE has conducted course evaluations. (www.acenet.edu/nationalguide) The Council on Occupational Education (COE) accreditation seal and the ACE logo have been added to the CDSE webpages, and the ACE logo has also been added to the course descriptions in the Security Training, Education and Professionalization Portal (STEPP).

CDSE is also marketing the availability of these courses through various media sources across the defense security industry.

CDSE plans to submit the following courses to ACE for evaluation during FY12 and FY13.

FY12:

- DoD Security Specialist
- DoD Personnel Security Adjudications
- DoD Personnel Security Management for Security Professionals
- Special Access Programs 2nd Tier Review
- DoD Advanced Personnel Security Adjudications

FY13 (1ST QUARTER):

- Challenges in Analyzing and Managing Risk
- Security as an Integral Part of DoD Programs
- Statutory, Legal and Regulatory Basis of DoD Security Programs
- Understanding Adversaries and Threats to the United States and to the Department of Defense
- Writing and Communication Skills for Security Professionals
- Organizational Considerations in Applying Security within the Federal and DoD Bureaucracy
- Constitutional Law and its Application to DoD Security

ABOUT THE COURSES

FACILITY SECURITY OFFICER ORIENTATION FOR NON-POSSESSING FACILITIES CURRICULUM (ISO20.CU)

Two semester hours, lower-division baccalaureate/ associate degree category.

This program of study prepares individuals for the duties and responsibilities of a Facility Security Officer (FSO) in a contractor facility participating in the National Industrial Security Program (NISP). The FSO Orientation for FSOs at non-possessing facilities (facilities with no approved storage for classified material) curriculum complies with the training requirements stated in paragraph 3-102 of the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M). To be eligible to receive the college credits, students must complete all courses within the curriculum (13 courses).

FACILITY SECURITY OFFICER PROGRAM MANAGEMENT FOR POSSESSING FACILITIES (ISO30.CU)

Two semester hours, lower division baccalaureate/ associate degree category.

This program of study prepares individuals for the duties and responsibilities of a Facility Security Officer (FSO) in a contractor facility participating in the National Industrial Security Program (NISP). The FSO Program Management for FSOs at possessing facilities (facilities with approval to store classified material) curriculum complies with the training requirements stated in paragraph 3-102 of the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M). To be eligible to receive the college credits, students must complete all courses within the curriculum (17 courses).

INTRODUCTION TO SPECIAL ACCESS PROGRAMS (SA101.01)

Two semester hours, lower division baccalaureate/ associate degree category.

This course introduces students to Department of Defense (DoD) Special Access Programs (SAPs). The course describes the SAP environment and discusses the interaction among the executive, legislative, and judicial branches of Government in establishing SAP policy. The roles and responsibilities of oversight and support offices and agencies, and mandatory SAP requirements are reviewed. Lessons address security enhancements across security disciplines, compliance inspection requirements, annual reviews, compliance inspections, and audits. The target audience for the course is newly assigned SAP security professionals, SAP non-security professionals, and security professionals needing refresher training on SAP policy.

SPECIAL ACCESS PROGRAMS MID-LEVEL SECURITY MANAGEMENT (SA201.01)

Three semester hours, upper division baccalaureate degree category.

This course offers an in-depth explanation of Special Access Program (SAP) security management. The course focuses on student ability to determine enhanced security requirements based on threat and vulnerability of SAPs. Students are given scenarios to practice adjusting security countermeasures throughout SAP life cycle in response to the changing threat. Students review, revise, or write security-related supporting documentation such as treaty, physical security, and transportation plans. The target audience for this course is DoD civilian, military, and contractor personnel with multidiscipline responsibilities for the management, oversight, and support to DoD Special Access Programs with six months to three years' experience.

ALL HANDS MEETINGS REACH

To effectively communicate the message, "Right Assessment, Right Facility, Right Time," to its employees across the country, Industrial Security Field Operations (ISFO) held a number of training meetings this year.

The ISFO Supervisor's Training Meeting was held March 13-15, at the Russell-Knox Building, Quantico, Va. Employees of the Northern and Western Regions met at an all hands meeting in Phoenix, Ariz., from March 26-30, and the Capital and Southern Region employees met for an all hands meeting in Atlanta, Ga., from April 16-20.

The meeting agenda featured a variety of presentations and small-group training sessions on conducting threat based vulnerability assessments, case studies from the Operations Analysis Group and updates to the security rating matrix.

Stan Sims, DSS Director, opened the meetings, and addressed issues affecting DSS and steps the agency needs to take to be successful in the future. "I gave you a vision when I came here and you executed it," said Sims. "And I thank you for your work."

In particular, Sims noted the enhanced partnership DSS has achieved with industry and its much improved reputation with its government customers. "I think we've established a model of how DSS and industry can work together," he continued. "We are here to help industry fix problems; we are not here to put them out of business."

In spite of the DSS successes of the past year, Sims promised the audiences more change. "Our mission will not change," he emphasized, "but there will be fundamental change in how we do our mission."

In particular, Sims predicted a more cyber-focused workload as well as a more global corporate environment. The challenge for the agency, he said, is in defining the agency's workforce of the future and would require active workforce management. For instance, he expects all Industrial Security Representatives to have some basic information technology training in the future.

He concluded by challenging employees to change something when they returned to their respective offices.

"We have to maintain relevancy within the Department of Defense," he said. "Your knowledge, skills and abilities must be different for the future. So we are going to change, and will continue to change and posture ourselves for 2016 and beyond."

Reginald Hyde, Deputy Under Secretary of Defense for Intelligence and Security, spoke to the audience in Phoenix and thanked DSS employees for their efforts to support the men and women in uniform. "You are the first line of

ACROSS THE COUNTRY

defense," he said. "Our technology – what gives us dominance on the battlefield – resides in industry and it is a target."

Timothy McQuiggan, director, Government Security, Boeing Defense, Space and Security, attended both all hands meetings and provided industry's perspective on DSS and the Industrial Security Program. In doing so, he listed the challenges faced by industry: a constant, persistent cyber threat, implementing an insider threat program and how to address huge losses of proprietary data.

"We want to be security professionals first," McQuiggan said. "Our Facility Security Officers overwhelmingly are trying hard and want to be recognized for doing well. But just as you have personnel challenges, we have FSOs with a wide range of experience."

"Our partnership is critical if we are to work together to find solutions," McQuiggan continued. "Partnership requires trust but it comes with some risk. However, collectively we are stronger. If we're at odds, everything is that much harder."

The Office of the Chief Information Officer (OCIO) manned a help desk at both all hands events and provided a variety of services to the meeting attendees. The DSS customers received technical support, training, and in some cases, replacement equipment. "Both sessions were very productive this year," said Kevin Baker, chief, Networks and Infrastructure, noting that in Phoenix, the team worked 160 information technology issues and questions, and in Atlanta, they worked 173.

"The OCIO team brought back candid feedback from customers, new ideas and suggestions on how to improve services, and a better understanding of how the agency operates and the unique challenges faced by our mobile workforce," said Baker.

Business Enterprise sent six individuals to each all hands meeting. The goal was for them to hear, first hand, what is going on in the agency and its direction, and understand their role in making the agency run. "This was a great opportunity for support personnel to 'own the mission' and tell the support story when possible," said Barry Sterling, director, Business Enterprise/Chief Financial Officer. "It allowed these individuals to acquire a greater understanding of the mission and see how what they do impacts the mission."

DSS EMPLOYEES ACHIEVE *Certification*

MANY ARE AMONG FIRST TO BE AWARDED SECURITY ASSET PROTECTION PROFESSIONAL CERTIFICATION

A ceremony held on April 5, 2012, at the Center for Development of Security Excellence (CDSE), recognized the DSS employees who most recently achieved certification under the Security Professional Education Development Program or SPēD. In addition to acknowledging the employees who achieved the first level of certification, Security Fundamentals Professional Certification (SFPC), DSS employees were among the first to achieve the second level of certification, Security Asset Protection Professional Certification (SAPPC).

The employees recognized represented the entire agency and included CDSE instructors, course curriculum developers, industrial security representatives, security specialists in Industrial Policy and Programs, and DSS' own Chief of Security. Due to the geographic dispersal of DSS employees, not all of the recent conferees were able to attend the ceremony; instead, field personnel were recognized at one of two all hands events held in March and April.

In presenting the certificates, Stan Sims, DSS Director, said the achievement by the DSS conferees shows that the agency is truly leading this certification effort across the Department and walking the walk. "We can't be considered a 'Center of Excellence' for Security Education if we don't have 'excellent' people, doing 'excellent' work," he said. "And we can't be the lead liaison with cleared industry unless we have the best people engaged."

Sims' remarks focused on the importance of certification to the individual but also to the Department of Defense. "SPēD provides security professionals with a certification that is recognized and transferable throughout the Department," he said. "It validates security as a professional career field in the Department."

Sims likened SPēD certification to those obtained by other professional career fields – accounting, legal, dental and medical. "If you visit the dentist, you want to see his certificate on the wall. You want to know you're getting the best care possible. We are doing the same with the security field."

In discussing the certification exam, Sims noted that the passing rate is just under 50 percent for SFPC. He explained that the pass rate shows the exam is rigorous but passing is clearly achievable. "If everyone can pass the certification exam with little effort, then it doesn't have as much value," he said. "But it's clear that if you prepare and know your stuff, you can pass."

Denise Humphrey, the CDSE Deputy Director who also chairs the Defense Security Training Council (DSTC), addressed the audience. She thanked the members of the DSTC for their support of the program and efforts to turn the "dream" into a reality.

The DSTC was established in 2007 as an advisory body on DoD security training, responsible for promoting certification programs for the security workforce. It is composed of security professionals and managers from 24 DoD components and agencies.

Since its beta test launch in 2010, 2,623 DoD security professionals have taken the SFPC. Of that number, almost 1,200 have achieved a passing score.

The SAPPC beta test was launched at the DoD Worldwide Security Conference in August 2011, and concluded in November. Of the 293 who participated in the beta test, 189 received a passing score, which is a 65 percent pass rate.

The blueprint for the third certification under SPēD, Security Program Integration Professional Certification (SPIPC), has been accepted and beta testing should take place later this year.

DSS Conferees:

SFPC Conferees:

Treva Alexander, CDSE
Sara Ballard, Huntsville Field Office
Christine Beauregard, CDSE
Deborah Bourgeault, Andover Field Office
Joseph Campbell, Smyrna Field Office
Jeffery Cassil, Phoenix Field Office
Kimberly Clark, CDSE
George Goodwin, Industrial Policy and Programs
Denzil Hall, CDSE
Scott Harkema, Industrial Policy and Programs
Timothy Harrison, DSS Chief of Security
Donna Jarvis-Smith, CDSE
Tracy Kindle, Industrial Policy and Programs
Elita Lane, Maryland Field Office
Richard Norman, CDSE
James Perham, Industrial Policy and Programs
Ryan Piroutek, Phoenix Field Office
Kyla Power, Phoenix Field Office
Kathleen Roth, CDSE
Judith Schluter, CDSE
Rojohn Soriano, Seattle Field Office
Angela Steinmetz, CDSE
Natasha Wright, Industrial Policy and Programs

SAPPC Conferees:

Randy Akers, CDSE
Richard Avery, CDSE
Christine Beauregard, CDSE
Marc Brandsness, CDSE
George Goodwin, Industrial Policy and Programs
Walter Hayward, CDSE
Danny Jennings, CDSE
Amanda Johnston, CDSE
Patsy Mann, CDSE
Brian Miller, CDSE
Lisa Rainey, CDSE
Andrew Reyes, CDSE
Judith Schluter, CDSE
Glenn Stegall, CDSE
Angela Steinmetz, CDSE

Elita Lane (right), and Pamela Hunter, of the Maryland Field Office.

Conferees congratulate each other for achieving certification.

Adriene Brown, CDSE, cuts and serves cake.

DISCO, WORKING GROUP ADDRESS INDUSTRY ISSUES

The Defense Industrial Security Clearance Office (DISCO) plays a critical role in the National Industrial Security Program by adjudicating personnel security clearance eligibilities for contractor employees requiring access to classified information.

On average, DISCO receives between 14,000 and 16,000 personnel security clearance requests each month – either for initial investigations or for periodic reinvestigations. DISCO makes approximately 12,000 adjudicative decisions each month.

Given the high-volume workload at DISCO and the importance of its mission to cleared industry, Chuck Tench of the DISCO Planning Office and Quinton Wilkes (L-3 Communications Corporation), representing NCMS, established a DSS/Industry Working Group to provide a forum to elevate issues related to processing personnel security clearances, inform industry stakeholders of pending changes to policies and processes, and establish a partnership for the future. (NCMS is a professional association established in 1964 to advance the practice of classification management in the disciplines of industrial security, information security, government designated unclassified information, and intellectual property.)

The working group began discussions in August 2011 with representatives from DSS, the NCMS core working team, the Defense Manpower Data Center (DMDC), and the Defense Information System for Security (DISS) Program Office. They have also invited guest speakers or subject matter experts from outside the working group to provide briefings on the development of initiatives affecting both DSS and industry.

One of the first issues the group dealt with were the moves mandated by the Base Realignment and Closure Commission, which directed DISCO's relocation from Columbus, Ohio, to Fort George G. Meade, Md. That move, completed in August 2011, resulted in the turnover of approximately 80 percent of DISCO's experienced adjudicative workforce.

The DoD Security Services (Call) Center also moved from Columbus, Ohio (and co-site in Alexandria, Va.), to Lorton, Va., resulting in a 75 percent turnover of customer service personnel.

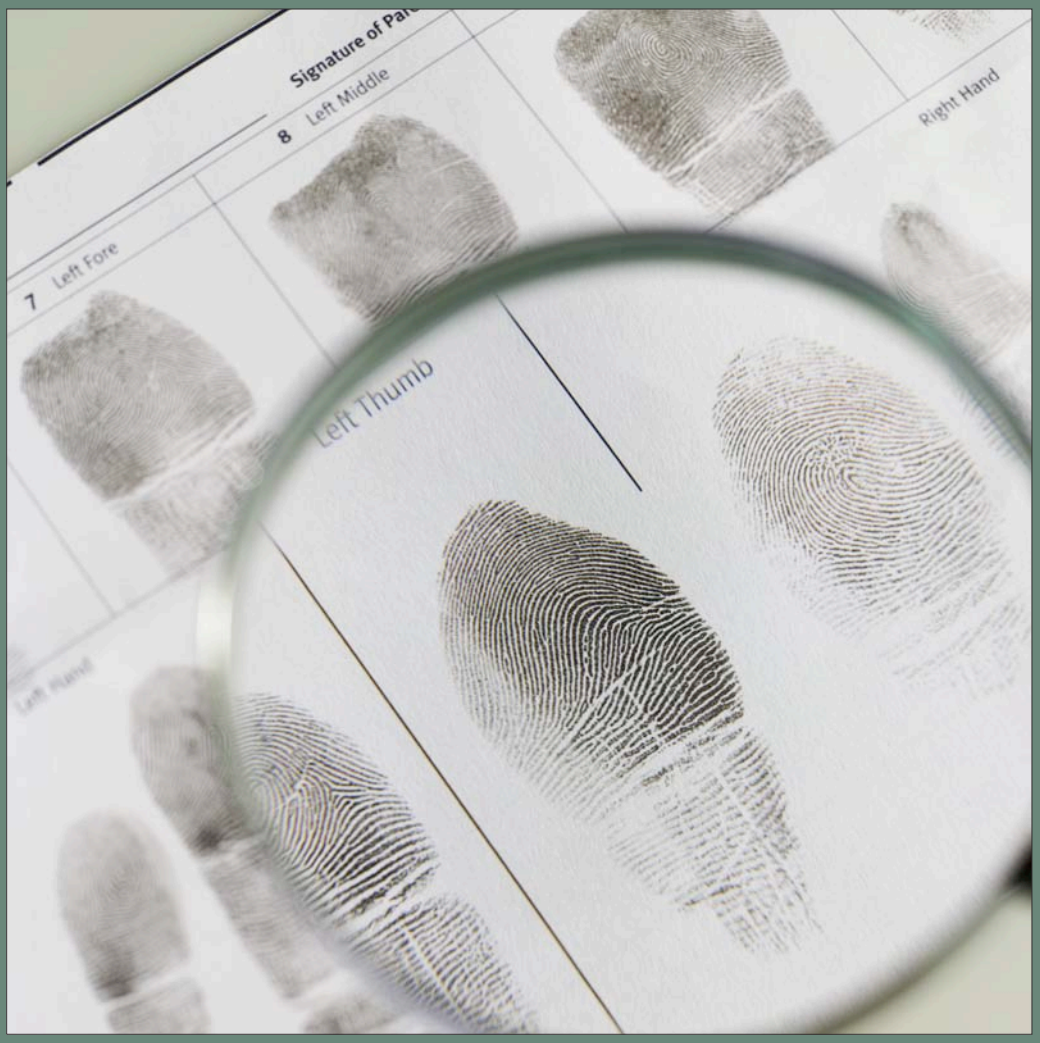
At about the same time, industry was adjusting to the mandate to begin using PKI (public key infrastructure) certificates to access the Joint Personnel Adjudication System (JPAS). JPAS is the Department of Defense automated system of record for personnel security eligibility and access information for DoD government, military and contractor personnel. Each industry company had to independently procure Personal Identification Verification (PIV) cards and ensure the certificates were compatible with JPAS.

All these issues had the potential to significantly affect, and possibly delay, the processing of personnel security clearance eligibilities for Industry personnel.

The working group holds monthly teleconferences; however, it held its first quarterly face-to-face meeting in October 2011. The face-to-face meetings typically span two days and allow the team to delve more deeply into unresolved issues and strategize on possible courses of action.

The main agenda item for October's meeting was the requirement for industry to submit electronic fingerprints as part of the clearance process and ways to make it more efficient. The group achieved consensus on how to expedite the movement of electronic fingerprints through the Secure Web Fingerprint Transmission (SWFT) Program for submission to the Office of Personnel Management (OPM) for quicker fingerprint check results.

The recommended changes to the software and submission process allowed fingerprints to be passed



SPEED UP THE PROCESS

The main agenda item for October's meeting was the requirement for industry to submit electronic fingerprints as part of the clearance process and ways to make it more efficient.

The group achieved consensus on how to expedite the movement of electronic fingerprints through the Secure Web Fingerprint Transmission Program for submission to the Office of Personnel Management for quicker fingerprint check results.

to OPM within two days, compared to four or more weeks in some cases.

The second face-to-face meeting was held in April 2012, and participation was expanded to include personnel from OPM and other internal DSS offices, as needed. The April agenda included an in-depth discussion on steps DISCO has taken to improve the submissions and response times for Research, Recertify, and Upgrade (RRU) requests. The RRU is a feature in JPAS that provides Industry Facility Security Officers (FSOs) an avenue to submit requests for action to DISCO relating to JPAS record edits, reciprocity, and personnel security processing actions.

The working group's objective for RRUs is to better route the industry request to the appropriate DISCO workforce for prompt action. The group is continuing to improve and standardize this process to gain efficiencies for industry and DISCO that will lead to faster processing.

Also on the April agenda were topics involving DoD Security Services (Call) Center operations, communications to industry, PSI submissions (processing), SF-86 (2010) issues, OPM rejects, and e-Fingerprints.

The DISCO Planning Office monitors action items that are identified and tasked during the DSS/Industry Working Group meetings, and a progress report on each action is briefed during the monthly teleconferences.

As the meetings continue to evolve, the DSS/Industry team will work together towards unprecedented improvements in the NISP personnel security process, systems, and most important, communication methods.

CEREMONY REMEMBERS 17TH ANNIVERSARY OF OKLAHOMA BOMBING

For a first time visitor, it's hard to imagine a nine-story building ever stood on the site of the Oklahoma City National Memorial and Museum in the heart of the city. A reflecting pool now interrupts 5th Street, the street that ran directly in front of the Alfred P. Murrah Federal Building. It was on 5th Street that Timothy McVeigh parked a Ryder truck packed with explosives that brought down the building on April 19, 1995.

The Field of Empty Chairs, one for each of those killed, is located within the footprint of the building. The chairs sit on a field of well-tended grass with trees now large enough to throw a late afternoon shadow. The Survivor Tree, a 90-year-old American Elm originally located in a parking lot across 5th Street from the building, survived the blast, but photos taken shortly after April 19, show it damaged and stripped of all vegetation. Today it not only has recovered but offers seeds that are grown as saplings for visitors to take home to plant and remember the victims.

Even the Survivor Wall, located on the east end of the Memorial and containing the only remaining walls of the Murrah Building, looks more a part of the surrounding landscape than the foundation of a structure that stood for 18 years.

Designed to offer comfort and quiet reflection, the Memorial does just that.

A ceremony held on April 19th, 2012, marked the 17th anniversary of the bombing and provided a stark reminder of the destruction wrought that day, of loved ones lost, and the lives forever changed.

As the crowd of approximately 2,000 began to gather, some placed flowers on the empty chairs, while the Edmond North High School Orchestra played in the background. Some attendees wore buttons with photos of loved ones as they were in 1995; the most striking were the photos of babies who would now be graduating from high school. Still others could be heard remembering what it was like at the site in 1995, where they were and what they were doing when the bomb went off.

A lone bag piper opened the ceremony by leading the procession of dignitaries, speakers and survivors to the stage. Following a brief welcome, at promptly 9:02 a.m., the exact time the bomb was detonated, the crowd observed 168 seconds of silence, one for each of the lives lost that day. Leading the observance was Christopher Nguyen, a survivor of the America's Kids Child Development Center, located on the second floor of the Murrah Building. Nguyen was one of only six children in the center who survived that day.

Nguyen was followed by Oklahoma City Mayor Mick Cornett, and Oklahoma Governor Mary Fallin, who in turn talked of the courage and resilience of the survivors, family members, the city and state. They also spoke of the first responders who established the "Oklahoma" model of response and interagency coordination now emulated by other cities and crisis response teams.

It was the words of Morgan Merrell, a two-year-old in 1995, whose mother, Frankie Ann Merrell perished in the third floor Federal Employees Credit Union, which perhaps best captured the reason for the annual ceremony. Merrell talked about growing up with the only memories of her mother coming from others. The experience prompted her to become involved in the Memorial to ensure the victims would always be remembered. "It's not all about grieving," she said, "but about remembering."

To ensure Merrell's mother and the other victims were remembered, a succession of speakers then read the names of the victims, names which were punctuated with "brother," "son," "mother," "sister." Those names included the five employees of the then Defense Investigative Service who perished on the third floor of the building: Harley R. Cottingham, Peter L. DeMaster, Norma "Jean" Johnson, Larry L. Turner, and Robert G. Westberry.

As the crowd began to disperse, most drifted to the field of chairs — now covered in flowers. Each victim remembered.

LEFT The Field of Empty Chairs represents the 168 lives taken on April 19, 1995 in the Oklahoma City Bombing.

ABOVE Flowers and mementos are left on the chair of Norma Jean Johnson, one of five Defense Investigative Service employees who perished in the bombing; a lone bagpiper walks past one of the Gates of Time during the ceremony.

NOTE: DSS Chief of Staff Rebecca Allen and the Chief of Public Affairs Cindy McGovern represented the agency at this year's memorial ceremony. In addition to placing flowers on the five Empty Chairs, they met with family members of the DSS employees killed in the bombing.

NEXT CERTIFICATION LEVEL LAUNCHED; 193 PROFESSIONALS CONFERRED

In February 2012, the Center for Development of Security Excellence (CDSE) launched the Security Asset Protection Professional Certification (SAPPC) Assessment, the second of four certifications within the SPēD Certification Program. The SAPPC serves as an indicator of the ability to apply foundational security concepts, principles, and practices critical to successfully perform functions, implement programs, and pursue missions necessary to manage risks to and protect DoD assets.

To take the SAPPC assessment, a candidate must be a Security Fundamentals Professional Certification holder in good standing and be designated eligible by their employing DoD component. As of April 17, 2012, 193 security professionals had successfully passed the SAPPC assessment and were being conferred the SAPPC certification.

CDSE introduced a diagnostic tool on the CDSE website *http://www.dss.mil/seta/sped/diagnostic-tools.html* for candidates to review learning content and assess strengths and weaknesses on the test content. This document presents examples of scenarios presented on the test. Additionally, a listing of relevant Intelligence Community Directive 610 competencies, which align to the scenario and to existing learning content, is available for review. Finally, a list of topic questions is presented after each scenario to provide an orientation of what to expect during the actual examination.

CDSE is currently developing and expects to launch the remaining two certifications in the SPēD Certification Program: Security Program Integration Professional Certification (SPIPC) and Security Enterprise Professional Certification (SEPC), during FY13 and FY14 respectively.

TRAINING PRODUCT RECOGNIZED WITH PRESTIGIOUS LEARNING AWARD

The Storage Containers and Facilities practical exercise won a Bronze Excellence in Learning Award from Brandon Hall in the Best Custom Content category. The exercise is part of the physical training curriculum offered by the Center for Development of Security Excellence. This course is an interactive web-based course that provides an overview of the approved security containers and facilities used in the protection of classified national security information as well as other sensitive Department of Defense assets. The course identifies:

- The types of General Services Administration (GSA) approved security containers and their uses
- The labeling requirements for GSA-approved security containers
- The types of restricted areas and their uses
- The physical security requirements for secure rooms, vaults, and Sensitive Compartmented Information Facilities
- The storage requirements for Arms Ammunition and Explosives and nuclear weapons
- The best practices and requirements for use of security containers and facilities

Now entering its 18th year, the Brandon Hall Group Excellence Awards Program is the most prestigious awards program in the industry. Pioneered in 1994 and often called the "Academy Awards" by learning, talent and business executives, the program was one of the first of its kind in the learning industry. In the last several years, they have expanded to include additional categories that cover functional areas responsible for driving performance within an organization. Brandon Hall recognizes the best companies that have successfully developed and deployed programs, strategies, modalities, processes, systems, and tools that have helped companies achieve measurable results.

Brandon Hall awards winners based on three levels: Gold, Silver and Bronze. In past years, 20 percent of the entries have won awards. In 2011, there were 89 winners from the Excellence in Learning categories.

INTERNATIONAL DIVISION OVERSEES INDUSTRY INVOLVEMENT WITH FOREIGN GOVERNMENTS

After World War II, the U.S. government authorized exports of defense technology to preserve national security, expand foreign policy, and build the economy through foreign commerce. Since then, the United States has been opening the export doors ever wider, allowing increasing amounts of high technology beyond its borders. This push allows the Joint Chiefs of Staff to achieve its military objectives, and further allows U.S. companies to be more competitive in the world market.

The expansion of technology exports with international programs has a two-fold effect: it increases the nation's industrial base by bringing in funds and ideas that support the economy, but it also creates foreign competitors of the same products and procedures being exported. Although the sharing of technologies brings allies closer together in regard to military defense, it also increases the opportunity for technology compromises that jeopardize national security.

International programs are a lawful and authorized effort in which there is a contributing or receiving foreign participant and information is transferred from one country to another and can be categorized as commercial or government. Commercial transfers occur during Direct Commercial Sales (DCS) — usually initiated by a U.S. contractor to sell controlled defense articles or services. Government transfers arise from Foreign Military Sales where the U.S. Government sells a defense product to a foreign government. Both types of sales require strict adherence to security protocols for the protection of classified information.

The International Division of Industrial Policy and Programs provides security and administrative oversight of exports resulting from DCS by U.S. defense contractors to foreign governments and foreign contractors, to include permanent and temporary imports of classified information in compliance with security agreements.

"We coordinate and approve approximately two shipments of classified information each day, every day," said Richard Stahl, chief of the International Division. "We have consistently seen a 25 percent increase over the past three years, with 370 shipments in 2010, 460 in 2011, and are on track to approve 572 in 2012."

"WE COORDINATE AND APPROVE APPROXIMATELY TWO SHIPMENTS OF CLASSIFIED INFORMATION EACH DAY, EVERY DAY"

RICHARD STAHL
CHIEF, INTERNATIONAL DIVISION

"The United States is bound by international laws and treaties to uphold bilateral agreements established between our governments," Stahl continued. "If DSS International did not perform its requirement of coordination, approval and oversight for the movement of classified information between the United States and 68 plus foreign governments, we would be in violation of those laws and treaties."

The division also represents DSS in international matters, such as meetings, conferences, and visits to other countries conducted under the National Disclosure Policy Committee (NDPC) and represents DSS in supporting the negotiation of international industrial security arrangements with other governments. Finally, the office plays a key role as liaison to foreign government security officials, other government organizations, and corporate international offices.

This liaison forms the framework for functions, such as:

- Establishing government-to-government channels for subsequent exchanges of assurances;
- Approving security arrangements (i.e. hand carriage plans, transportation plans approvals) on behalf of the U.S. and coordinating these approvals with foreign governments and NATO; and
- Requesting classification guidance and evaluating compromise reports involving foreign government or NATO information and providing notification to the originating foreign governments.

THE GREAT IMPOSTER

EVENT DETAILS

In August 2011, an individual (subject) claiming to be a senior executive of a large cleared contractor (company A) contacted a mid-sized cleared contractor (company B) by telephone and requested to be transferred to a specific key manager. The subject was transferred to the requested individual and advised him that he had been referred by another manager at company A. The subject stated that he needed to meet with the manager immediately to discuss a time-sensitive program.

The subject was very insistent that the meeting needed to take place "that day" and that the "meeting was time-sensitive."

A meeting was arranged and when the subject arrived at company B that afternoon, he presented a business card that appeared to be from his company. He stated that he was the only person in his company who was supporting the selection of company B in an ongoing competitive bid process.

When asked about the specifics of his requirements and the competition, the subject stated that "he could not provide them because the details were classified."

Prior to the beginning of the discussion, the subject asked company B's employees whether they had security clearances. They informed the subject that one of the employees did not and that the room they were in was not cleared for classified discussions.

The subject stated that he "could describe things in an unclassified way." He then described a memorandum of agreement between multiple federal agencies: the Department of Homeland Security, the Defense Intelligence Agency, the Defense Threat Reduction Agency, and U.S. Immigration and Customs Enforcement.

The subject stated that these agencies were looking for a solution to a specific problem concerning "bad guys." The subject further stated that a meeting was scheduled at his office, in a SCIF (Sensitive Compartmented Information Facility), the following week, and that representatives of a competitor of company B would be present.

The subject stated that he "was the only person pushing for company B and that the decision makers wanted to go with the competitor."

The subject requested a demo portraying a specific scenario that could be shown as a movie or run live on a laptop or mobile device provided by company B. Company B employees presented a few different applications demonstrating some of the capabilities of their products. Company B employees did not display any proprietary or sensitive workflows. All the demonstrations were standard marketing demos that had no data restrictions or security concerns.

At the subject's request, company B created multiple variations of the software capabilities and loaded three videos demonstrating these capabilities onto a thumb drive the subject provided. The subject was permitted to use the restroom facilities without an escort. Before leaving company B, the subject asked for a "rugged device" that he could use to display the videos in his SCIF the following week. The subject insisted that using their rugged device would give company B an edge over their competitor. The company did not provide the requested device.

Once the meeting concluded, the employees reported the subject's behavior to the key manager as suspicious. The company's information systems security manager removed the computer into which the subject had plugged his thumb drive, ran several virus scans, and reviewed firewall logs. The scans did not detect anything harmful.

Further inquiry by Defense Security Service (DSS) confirmed that, while the individual had previously

been an employee of company A, he no longer held a position there. In fact, he had resigned under the cloud of an ongoing fraud investigation. Company A had terminated the subject's employment but did not enter an incident report in JPAS (Joint Personnel Adjudication System).

Five months later, when company A found the subject culpable for misconduct based on the fraud investigation, they reassumed ownership of the subject's clearance and placed an incident report in JPAS.

LESSONS LEARNED

- Company B took appropriate action by reporting the suspicious contact to DSS.
- Company B employees allowed an individual, whose identity and claimed employment they had not confirmed, to enter their facility.
- Company B employees introduced a thumb drive into their information technology system without properly scanning the thumb drive for malicious code.
- Employees should periodically review their operations security responsibilities.
- Employees should periodically review their information assurance security responsibilities.
- These reviews should include training on restrictions on the introduction of removable media devices into, and their use on, company networks.
- Employees would benefit from counterintelligence awareness training, including the awareness of social engineering techniques and tactics.

OUTCOMES

This individual had been the subject of a previous JPAS incident report and his access to classified information had been suspended for representing himself as a person with a security clearance when he was not.

The subject's conduct related to his meeting at company B has been referred to Federal law enforcement agencies for investigation.

>> BEFORE & AFTER

A TALE OF TWO SECURITY PROGRAMS

By Bart Cawley
Field Office Chief, Boston Field Office

With apologies to Charles Dickens, it was the best of times, it was the worst of times, and this really is a tale of two security programs. The facility is an engineering and manufacturing company that has a Secret facility clearance (FCL) with Secret safeguarding capability. This facility is also a non-signatory corporation under a Proxy Agreement.

In 2010 DSS assigned an unsatisfactory security rating (the lowest possible rating) to this facility because of three serious vulnerabilities and four administrative vulnerabilities. In 2012, the same facility received a Superior security rating (the highest possible rating) from DSS. In just two years, this facility was able to turn around its security posture.

During the 2010 assessment, DSS found one serious vulnerability that involved processing classified material on two information systems (IS) after the IS accreditation had expired. The assigned Industrial Security Representative and the Field Office Chief had notified the facility security staff and the senior management official on five occasions that their IS accreditation was expiring and the systems could not be used to process classified material after the accreditation had expired.

The security staff failed to properly notify all users and follow through with appropriate actions to ensure that neither IS was used after the accreditation had expired.

The second serious vulnerability involved an employee with a confidential clearance retrieving a package from a U.S. Post Office that contained secret material.

The third serious vulnerability was repeat IS findings that show audit log analysis was not conducted and the IS were not configured for auditing of unsuccessful access to security-relevant objects (authentication data and archived audit data).

When DSS assessed the facility in 2012, the facility had fully implemented the requirements of the National Industrial Security Program Operating Manual (NISPOM) in an effective fashion, resulting in an exemplary security posture. This rating was assigned because the security program now has strong management support, the absence of any serious security issues and during the vulnerability assessment, only one vulnerability was noted. The facility continues to show strong improvement since its unsatisfactory rating.

The facility's success can also be traced to excellent management support from the corporate office, especially as it related to the administration and oversight of the Proxy Agreement. The facility implements an automated system to use for Requests for Interactions and Unplanned Contact Reports, and has many impressive auditing functions as well.

The corporate office also continues to provide training and oversight of the Proxy Security requirements to include "peer review" audits. The corporate Facility Security Officer (FSO) assigned three security professionals from other corporate facilities to attend the latest assessment and assist local staff where possible.

The overall superior assessment of the facility's security program was due to receiving credit for 12 of 13 "NISP related security enhancements". All enhancements were verified by DSS during its assessment.

In addition to the NISP enhancements, the following areas of the facility's security program were also recognized as exemplary and clear indicators of a superior security posture:

- The amount and type of NISP-related training the FSO had completed in a short time
- The administrative termination of 10 personnel security clearance eligibilities in 2011 that were no longer needed
- All periodic reinvestigations for the facility were up to date
- The annual justifications of the requirement for personnel security clearance eligibilities
- Perimeter controls, practices, and procedures
- A significant reduction in the number of classified documents that were no longer associated with a classified contract
- Employee awareness of requirements under the Proxy Agreement and Special Security Agreement
- No vulnerabilities identified in audits of information systems during this assessment
- All accredited information system hardware is labeled with the date the Interim Authority to Operate (IATO) or Authority to Operate (ATO) expires to help ensure no unaccredited processing occurs. Processing on an unaccredited system was a major factor in assigning an unsatisfactory security rating in 2010.

IN 2010 DSS ASSIGNED AN UNSATISFACTORY SECURITY RATING TO THIS FACILITY BECAUSE OF THREE SERIOUS VULNERABILITIES AND FOUR ADMINISTRATIVE VULNERABILITIES ...

IN JUST TWO YEARS, THIS FACILITY WAS ABLE TO TURN AROUND ITS SECURITY POSTURE.

- Information system maintenance logs have comprehensive detail on all recorded actions
- All information system user briefings note the date that the user is due for a periodic reinvestigation.
- A number of employees were recognized as having extraordinary security awareness

Again taking literary license, this is the best of times for this security program and well deserved.

DSS EMPLOYEE AWARDED LEGION OF MERIT

Marine Corps Chief Warrant Officer 5 Thomas J. Montero and his family stand on the deck of the U.S.S. Missouri in Pearl Harbor, Hawaii.

Thomas J. Montero, Counterintelligence Chief of Operations, Western Region, was awarded the Legion of Merit (LOM) at his retirement from the U.S. Marine Corps Reserve on Feb. 22, 2012, after 31 years of service.

Montero, who retired as a Chief Warrant Officer 5, was awarded the LOM for exceptionally meritorious conduct in the performance of outstanding service from January 2003 to February 2012.

"As long as I can remember I have always felt a deep desire to serve my country, though after joining the Marine Corps at the age of 20, I never thought I'd be in uniform for 31 years," Montero said. "My brothers in the Corps made me feel at home… it was the right service… the right fit for me which allowed me to fulfill my goal of serving my country."

As a decorated combat veteran, Montero served in a variety of intelligence, command, and staff positions at multiple levels stateside and abroad. Montero began his military career in the early 1980s as a Marine Corps infantryman and later switched to the intelligence field, participating in training exercises and real world operations in Latin America, Asia, and Africa. Through the late 1990s, he supported counterdrug, counterterrorism, and counterintelligence operations while assigned to the Defense Human Intelligence (HUMINT) Service, Office of Naval Intelligence, and other government agencies in Latin America and stateside.

He later deployed to Bosnia as a member of the NATO Allied Military Intelligence Battalion, and served as an attaché and operations coordinator in various U.S. embassies.

Soon after Sept. 11, 2001, he served as the senior leader of the Marine Forces Reserve Anti-Terrorism Force Protection (AT/FP) unit that successfully conducted vulnerability assessments throughout the United States. He also held the position of senior staff CI/HUMINT Officer supporting Marine Forces Pacific, where he was a key advisor on AT/FP issues affecting personnel in the Middle East and Pacific area of operations.

"My experience in the Marine Corps directly translates to my current position as the DSS West Region Chief of Counterintelligence Operations," Montero said.

In addition to the Legion of Merit, Montero is the recipient of 30 military awards, to include the Bronze Star, and numerous service and joint service commendation and achievement medals and certificates.

NEW LEADERS IN SOUTHERN REGION

Two key leadership positions were filled in the Southern Region recently: Regina Johnson was named the Regional Director and Ron Donley was named the Regional Designated Approving Authority. Johnson assumed her duties on May 7, 2012, and Donley on April 8, 2012.

REGINA JOHNSON

As the new director, Southern Region, Johnson is responsible for the region's industrial security oversight of nearly 3,300 National Industrial Security Program (NISP) facilities dispersed across a 14-state area, Puerto Rico, and the U.S. Virgin Islands. The region includes six field offices located in Irving and San Antonio, Texas; Huntsville, Ala.; Atlanta, Ga.; Virginia Beach, Va.; and Melbourne, Fla.

Johnson has been with DSS (and its predecessor, the Defense Investigative Service) since 1986 when she was a special agent conducting personnel security investigations. Prior to that, she worked at the Internal Revenue Service, Department of the Navy and Office of Personnel Management.

Johnson moved to industrial security in 1989 when she was selected as a DSS Industrial Security Specialist in the Houston Resident Office. During this time, she also served collateral duties as an Equal Employment Opportunity counselor and Foreign Ownership Control or Influence (FOCI) action officer.

In 2008, Johnson was selected as the Field Office Chief for the Irving Field Office, which provides oversight to companies in North Texas, Arkansas and Oklahoma. As the Field Office Chief, she served as the co-chairman of the DSS ISFO Implementation of Team Concepts and Team Integration Working Group, as well as the Facility Categorization and eFCL Working Groups.

Johnson is a board member of the Dallas/Fort Worth chapter of the Joint Security Awareness Council. She holds a master's degree in Public Administration from Texas Southern University and a bachelor's degree in Psychology from the University of North Texas.

RON DONLEY

As Regional Designated Approving Authority, Donley is responsible for implementing the National Industrial Security Program certification and accreditation program across the Southern Region. This includes strengthening existing and building new partnerships with government agencies and industry.

Prior to being selected as the Southern Region RDAA, Donley served as an Information Systems Security Professional team leader for the Western Region, working from the DSS office in Tucson, Ariz., for four years. Donley retired from the Air Force having served 21 years as an Aircraft Weapons System Specialist; Master Technical Training Instructor; Flight Chief; Quality Assurance Inspector; Team Member of the U.S. Air Forces Europe Inspector General; and First Sergeant.

Shortly after his retirement, Donley returned to college and earned a Computer Information System Management degree with honors. In 1998, he joined DSS as a Computer Support Technician in the Colorado Springs Field Office. In 2003, he accepted a position as an Information System Security Professional (ISSP) and relocated to Tucson, Ariz. As an ISSP, he provided oversight to cleared defense contractors in Arizona, New Mexico, and West Texas. In 2008, he was selected as team lead. Donley also completed a 6-month detail at DSS Headquarters as the Acting Assistant Deputy Director ODAA from 2009 to 2010.

Donley holds a bachelor of science degree in Computer Information Systems Management and an associate in applied science degree in Personal Management. He is a Certified Information System Security Professional and holds technical certifications in Security + and A+.

An airboat, piloted by a member of the Airboat Association of Florida, skims wounded warriors and their families across the Everglades.

A DAY IN THE EVERGLADES RECOGNIZES NATIONAL HEROES

Ciria Cruz, Industrial Security Representative in the Homestead, Fla., Office organized "A Day in the Everglades" for 200 wounded warriors and their caregivers. The February event featured airboat rides, food and live entertainment, and was hosted by the Air Boat Association of Florida (AAOF).

Cruz, who is an AAOF member, acted as chairperson for the event. She did some research and discovered that 10,000 wounded warriors are registered with the Veterans Administration (VA) Hospital in Miami. In trying to scale that number to the target attendance, she contacted the VA Hospital rehabilitation coordinator and the Army Wounded Warriors Program in Florida to get assistance in setting the criteria for attendance at the event. "I thought it would be better if the VA determined which veterans would most benefit from the event," Cruz said.

She next focused on organizing the volunteer efforts and formed several committees, each with a different task. One group contacted the local airboat groups in South Florida, who in turn donated their time and boats for the day. Some boats were fitted with wheelchair access, while other boats accommodated 20 non-wheelchair guests. On the day of the event, hour-long rides started at 10 a.m. and ran through 5 p.m.

Another volunteer group was in charge of coordinating a lunch for the guests, and received donations of food and refreshments from local restaurants and distributors. A third group put together a raffle for the wounded warrior guests, which featured donated items such as backcountry fishing charters, hog hunts, and tickets for Miami Heat basketball and Miami Dolphin football games.

Additional volunteers ensured the club grounds were groomed prior to the event, and orchestrated parking on event day. Cruz contacted local businesses for additional activities, and firearms, archery and hunting outfitters were on hand to demonstrate the latest equipment for use by physically challenged sportsmen, and a band provided live entertainment.

"An event such as this does not come together without the support of the entire group," Cruz said. "It must have been a success, because the (AAOF) club members and the VA are both calling to find out when we can do it again."

ISOO RIDES ALONG

OBSERVES CAPITAL REGION SECURITY ASSESSMENTS

Field offices in the Capital Region are hosting employees of the Information Security Oversight Office (ISOO) on "ride alongs" to cleared facilities to observe the security assessment process implemented by DSS.

The concept sprang from a DSS mission briefing, when Greg Pannoni, ISOO Associate Director, and David Best, Senior Program Analyst, ISSO Operations and Industrial Security Branch, expressed interest in observing various types of security vulnerability assessments.

"They're mainly interested in the pre-assessment research we do and then the actual conduct of the assessment, including follow up actions associated with vulnerability mitigation," said Doug Stone, acting Regional Operations Manager in the Capital Region.

The first ISOO ride along took place in March 2012 with a security vulnerability assessment team from the Chantilly Field Office. Leading the team was senior Industrial Security Representative Randy Stacey, who coordinated the observation of assessments for two companies in Virginia. Other members of the assessment team were Stone and Steve Durant, Sean Whitis and Ursula Stearns, all from the Chantilly office.

The ISOO is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program (NISP). ISOO is a component of the National Archives and Records Administration and receives policy and program guidance from the National Security Council. The Director, ISOO, chairs the National Industrial Security Program Policy Advisory Committee (NISPPAC), the national forum for all participants in the NISP, both government and industry, to discuss NISP policy issues.

"As members of the NISPPAC, we work closely with the ISOO staff, and we're pleased to have them observe first-hand the way we carry out our NISP oversight mission," said Kathy Branch, chief of the Policy Division, Industrial Policy and Programs. "Our assessment processes are an excellent model for ISOO's oversight of classified information in executive branch agencies."

Members of the Chantilly Field Office security assessment team (from left) Douglas Stone, Sean Whitis, Randall Stacey, Ursula Stearns and Steve Durant stand outside the National Archives.

The goal for ISOO is to take the information gleaned from the experience, and develop its own security assessment process, according to Best. The program is also advantageous to DSS, as it gives DSS "the opportunity to showcase our unique partnership between the agency and industry," said Stone.

"The initial review proved very fruitful and informative," Best said. "We were able to get some very useful information from the company employees regarding their knowledge of the NISP and their perspectives on dealings with classified information. We look forward to a very productive and continuing relationship with DSS."

Before any observer ride along can take place, the company's key management personnel and the facility security officer are contacted by the industrial security representative to brief them about the ISOO and the ride along program. If facility personnel express any issues, then the observation is scheduled for a different facility.

"To date, no facility has had any issues and all have welcomed the participation," Stone said.

Additionally, ISOO offered to allow a Capital Region action officer to participate in a familiarization exchange. In the future, Stearns will spend time with ISOO to observe its mission in relation to industrial security. Future opportunities for ISOO ride alongs will continue through the remainder of FY12.

NCMS OPENS QUANTICO CHAPTER

DSS DIRECTOR SPEAKS AT INAUGURAL MEETING

Managing security vulnerabilities and the threats of the future were a few of the topics discussed at the inaugural meeting of the Quantico Chapter of NCMS in early March, in Stafford, Va.

After opening remarks by Brian Price, NCMS Quantico Chapter Chairperson, Tony Ingenito, NCMS President, spoke about the importance of NCMS and the development of the new chapter. More than 100 people attended the meeting.

The purpose of NCMS is to advance the practice of classification management in the disciplines of industrial security, information security, government designated unclassified information, and intellectual property, and to foster the highest qualities of security professionalism among its members.

Stan Sims, Director DSS, commended NCMS for staying relevant within the security environment and provided an update on DSS initiatives.

"NCMS has expanded with the national security environment, and is on the leading edge," Sims said. "We need professionals to do professional work, which is why NCMS is so important."

In discussing DSS initiatives, Sims addressed agency efforts to improve the partnership with industry. "We have mutually supporting missions. National security is not served unless industry wins. We've got to find ways to better improve this partnership, so I ask that you help us get it right," Sims said. "I can make the best impact on national security by helping you do your job, and helping you succeed."

Topics of discussion included the new security ratings matrix launched by DSS, the new approach to prioritizing assessments, and the new terminology associated with those security reviews and vulnerability assessments. "In the past, we haven't put enough emphasis on the threat," Sims said, "and I think that needs to change. If we don't stop countries from stealing our intellectual property, then we won't be one of the most powerful nations in 20 to 30 years."

An outcome of the new security reviews is identifying vulnerabilities. "DSS will assess your security posture, determine the vulnerabilities and then share the information with you so that you're more aware of the threats," he continued. "The end result is that we operate ahead of the threat, not behind the vulnerabilities."

In looking toward the future, Sims predicted that 10 years from now, the cyber domain will define the security environment. To better handle the future risks, DSS will hire more Information Systems Security Professionals, and will expand their training to better understand and mitigate cyber vulnerabilities. Additionally, Sims has asked the Center for Development of Security Excellence to expand the curriculum for new Industrial Security Representatives to include training on recognizing cyber threats.

After his presentation, Sims took questions on topics ranging from the status of the National Industrial Security Program Operating Manual revision to industrial security-related training.

In closing, Sims said, "I understand where NCMS fits in the security world, and I encourage those who aren't members to join this organization. One of the benefits is that it will help you stay in touch with security."

HANOVER FIELD OFFICES GET MOVING

EMPLOYEES SHED POUNDS AND MOVE TO NEW LOCATION

By Jamie Davis
Hanover Field Office

The Maryland North and South Field Offices have gone through several changes this past year. There is a new Field Office Chief and the addition of an Operation Warfighter intern to the office. The collocated offices also relocated from Linthicum to Hanover, Md., in August 2011. However, there is another change that is quite obvious if you were to visit the Hanover offices.

For over a year now, several DSS personnel have taken on another mission: weight loss. The employees of the Hanover Field Office have joined others around the world fighting the obesity epidemic and have a success story of their own.

"I'm so tired all of the time;" "I can't fit in any of my clothes;" "I can't look at myself in the mirror;" or "I am so out of shape," were some of the reasons why one DSS employee decided that it was time to do "battle with the bulge." A few months later and a few inches smaller, employees started noticing and asking how she'd done it. Over the next several months, more employees started some type of weight loss plan and shared in the success.

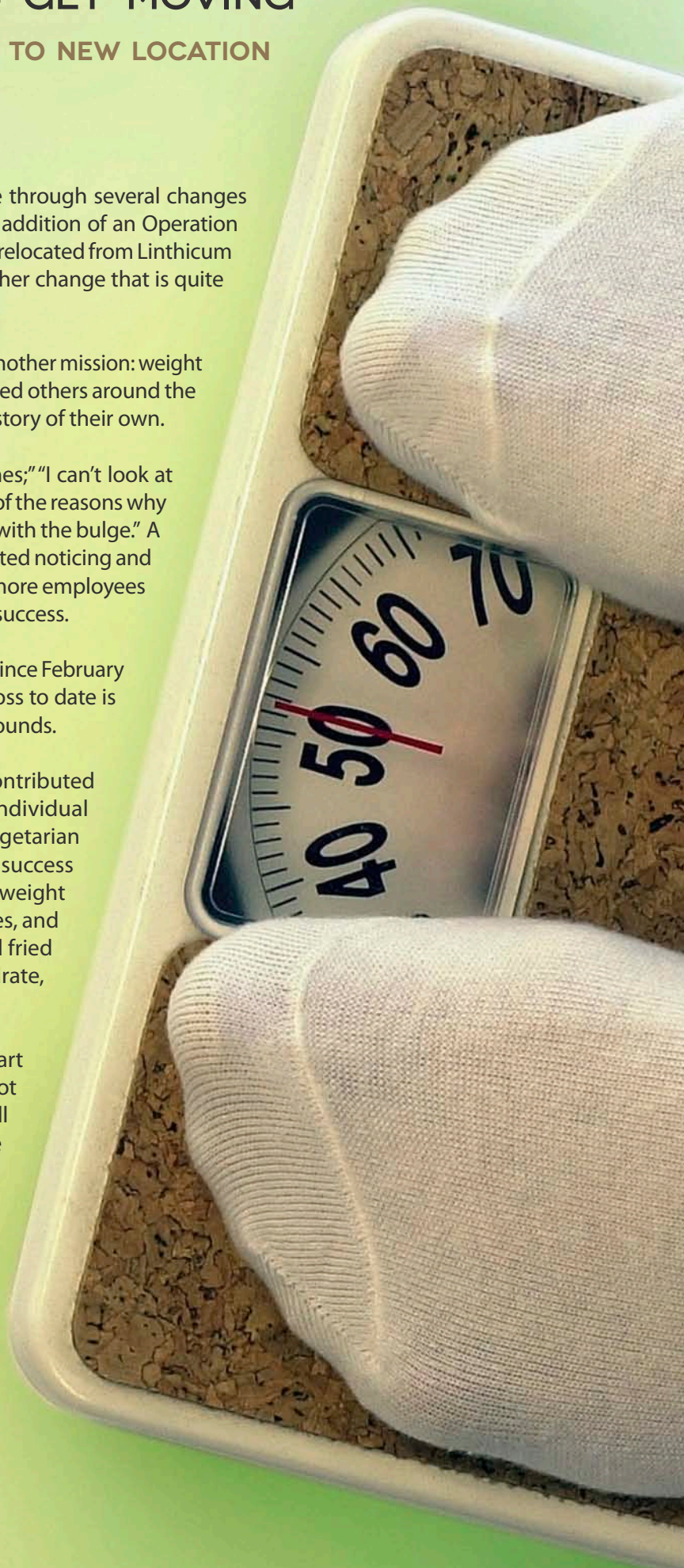
The total number of pounds lost by the collocated offices since February 2011 is an admirable 360 pounds. The average weight loss to date is 30 pounds with individual results varying from 5 to 65 pounds.

Ten DSS employees and two administrative assistants contributed to the total weight loss; all by following their own individual program. Some attribute their success to following a vegetarian diet, eating foods from the earth. One employee found success joining the Jenny Craig program with her husband (total weight loss between them — 94 pounds!). Others count calories, and have given up French fries, all fast foods, juice, soda and fried foods. Lastly, several people followed a low-carbohydrate, low-sugar diet.

Employees also adopted a regular exercise program as part of their healthy lifestyle. Running, biking, attending a boot camp every day at 5 a.m., walking, playing basketball and tennis are a few of the favorite activities among the Hanover Office personnel.

In addition to losing weight, employees also report improved blood pressure, lower results when tested for diabetes and cholesterol, a decrease in allergies, and a boost in self-confidence.

DSS is a very busy, dynamic agency, and the mission doesn't come without stress. But the Hanover Field Office has set the tone with proper dieting and exercise, and has a message to share with everyone … weight loss is contagious!




DEFENSE SECURITY SERVICE
UNITED STATES OF AMERICA