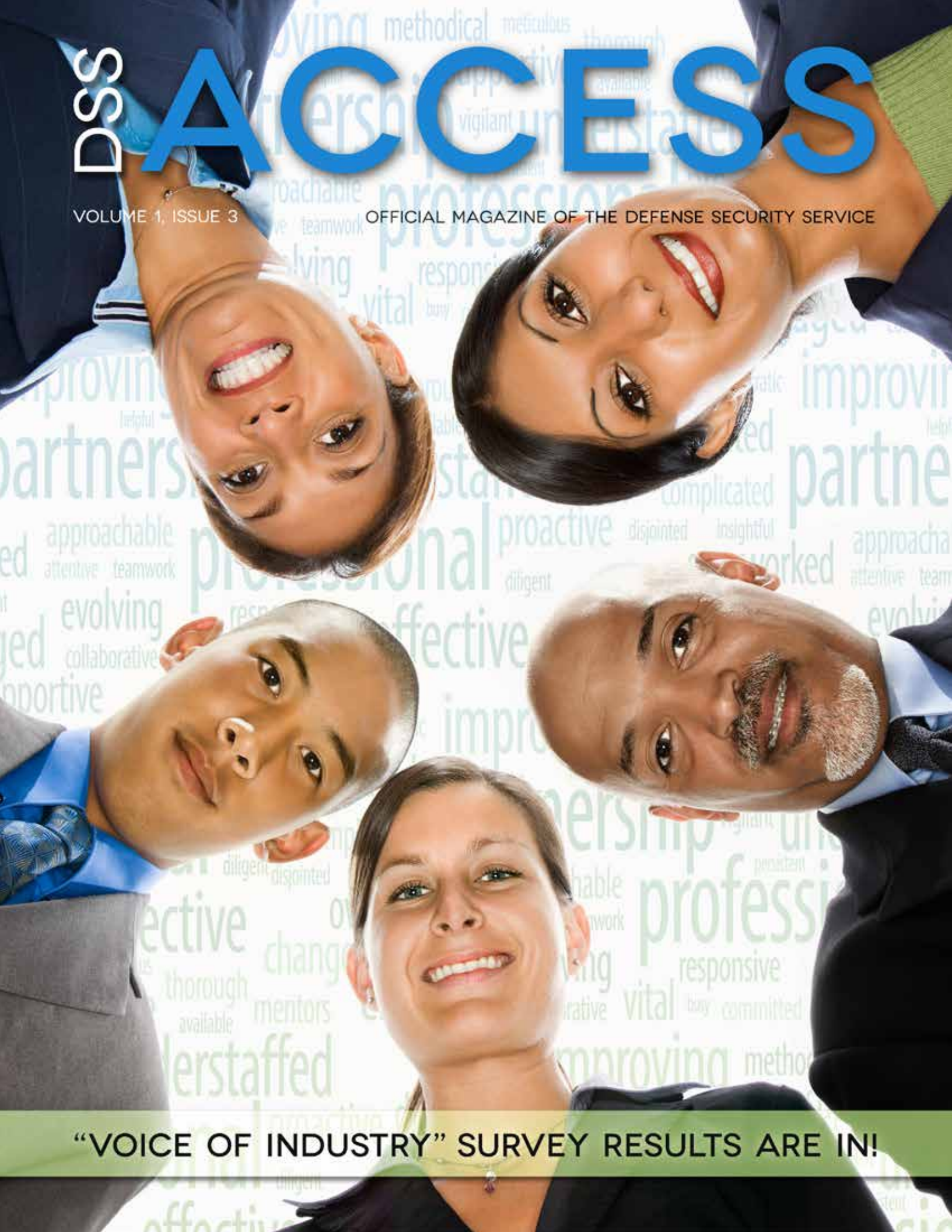
DSS ACCESS

VOLUME 1, ISSUE 3

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE



"VOICE OF INDUSTRY" SURVEY RESULTS ARE IN!

FALL 2012

VOLUME 1, ISSUE 3

SPOTLIGHT

INSIDE

DSS CASE STUDY

NEWS BRIEFS

AROUND THE REGIONS

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

Welcome to the DSS ACCESS Magazine. For returning readers, you will find this issue to be more introspective than the last two. In these pages we highlight the DSS employees who are going above and beyond in their professional and personal endeavors and achieving significant milestones. DSS employees are involved in their communities as volunteers. They serve, again voluntarily, on interagency working groups to contribute their expertise to find solutions across the security and intelligence enterprises. And they serve the nation as Reservists.

This issue also focuses on self-help, if you will. I'm pleased to provide a snapshot of the results of our annual Voice of Industry Survey. We solicit industry's feedback to adjust our communication methods, tweak our processes, and learn how we can improve the delivery of our services to industry. I believe we have made great strides in the past year in enhancing our partnership with industry, but there is always room for continued improvement. Please know that we do read the survey results, and we do pay attention to industry concerns.

To develop better leaders in DSS, we have initiated programs to expose our field personnel to other offices, different facilities, and slightly different ways of doing business. Our initial foray into this training is going well, and I'm anxious to expand these leadership training opportunities across the agency. In a time of budget and hiring constraints, we have an obligation to help ourselves in developing new methods of training but also in finding ways to provide opportunities for advancement for all employees.

Finally, we mark the 40th anniversary of the Defense Security Service. In looking back over the history and some of the earlier publications, I am struck by the fact that DSS is a vastly different organization than the one created in 1972. However, I am also struck by a column written by John Donnelly, Director from 1988 to 1996, who penned a 'Message from the Director' marking the agency's 20th anniversary. It's a column that is as relevant and telling as one I would write today. He noted the era of downsizing, a study of work requirements versus personnel assignments and the closing of smaller offices to cut costs. He discussed a high visibility acquisition of a cleared facility by a foreign-owned firm that prompted a "major review of FOCI [foreign ownership, control or influence] procedures." And finally, Mr. Donnelly talked about the importance of automation and how "we must seize the initiative to perform our mission in the most effective manner possible, while at the same time fulfilling our responsibilities to the security community."

After listing the significant challenges facing the Defense Investigative Service in 1992, John Donnelly closed his column by stating emphatically that "we WILL meet the challenges ahead." That he was able to face the future with such optimism is a testament to the professionalism of the people he had the honor to represent. I am as optimistic now as he was then for the same reason. As I said, this issue is introspective and highlights the good work being done at DSS by high-performing, dedicated people. While we continue to face significant challenges at our 40th anniversary, we also WILL meet the challenges ahead.

PARTNERSHIP COMMUNICATION

THE KEYS TO SUCCESS

VOICE OF INDUSTRY RESULTS ARE IN

Upon his arrival at the Defense Security Service in December 2010, Stan Sims, Director, stressed the need to nurture the partnership between DSS and cleared industry. He called for an open, transparent relationship and emphasized to the DSS workforce that it would be viewed on "how" it accomplished its mission.

The results of the second Voice of Industry Survey echoed Sims' philosophy and show an improving relationship between DSS, its field personnel, and their counterparts across industry.

The survey was sent to more than 13,000 Facility Security Offices (FSOs) of cleared industry in February 2012. The purpose of the survey was to pulse cleared industry to:

- Improve overall relations and customer service;
- Identify areas requiring improvement; and
- Evaluate whether DSS made progress since the baseline survey was conducted in fiscal year 2011.

Approximately 10,000 FSOs responded to the survey which provided a similar sample size to the 2011 survey. Overall the level of satisfaction with DSS has improved from 2011 to 2012 from 89 percent to 94 percent. Of the participants who noted changes in DSS processes over the last year, 48 percent had a positive response and only 3 percent had a negative response.

Richard Lawhorn, Director, Industrial Security Field Operations, was pleased to see the improvement in scores from last year and stressed, "We take the findings from the survey very seriously, and we strive to continuously improve the relationship between the agency and industry. By soliciting direct feedback from the FSOs, we can determine the most critical actions we must take that will have the most significant impact on our partners."

As with the initial baseline survey of 2011, several key themes emerged in this year's results:

- Frequency of interactions and duration of relationships had a significant impact on customer satisfaction levels
- Dissatisfied participants blamed inconsistencies

When respondents were asked to select one word that describes DSS, partnership and professional were most cited. However, it is important to note that words like overworked, understaffed, and complicated also surfaced.

between representatives with respect to interpretation of policy and assessment techniques

- Respondents indicated that DSS field personnel seemed overburdened, with limited capacity to meet the needs of industry
- Increased communication and expanded training and education offerings are key components to improving relationships with industry

The increase in satisfaction is linked to the improvements and changes made after conducting the 2011 baseline survey. Specific changes that have been rolled out based on the participants' feedback include: monthly newsletters, automated emails to notify FSOs of changes to representatives, and the security rating matrix.

Of the participants who noted changes in DSS processes over the last year, 40 percent mentioned the implementation of the new security rating matrix. This is particularly noteworthy as respondents were asked to "write in" a response, rather than selecting a choice from a drop-down or other menu.

The new matrix was introduced in the fall of 2011 and is designed to provide a numerically based, quantifiable means to capture all aspects of a facility's involvement in the National Industrial Security Program (NISP). While DSS continues to gather trend data and develop lessons learned, it is clear from the survey that the matrix provides more transparency to the rating process and that it has been well-received across industry.

Digging a little deeper, the survey found that 83 percent of respondents said they have a true partnership with DSS. Longer relationships between DSS representatives and industry personnel directly contributed to respondent satisfaction. For instance, FSOs who had been working with a DSS representative for six months expressed a 60 percent satisfaction rate. For those FSOs who had been working with a DSS representative for five years, the level of satisfaction increased to 80 percent.

Likewise, the frequency of communication had a significant impact on satisfaction levels, with 46 percent of responding FSOs indicating that DSS works with them at least monthly (versus 25 percent in 2011).

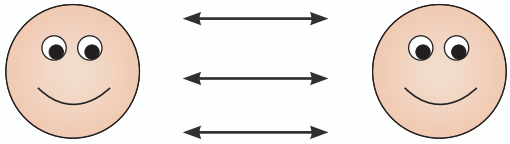
The survey measured FSOs' satisfaction levels with their Industrial Security Representatives, Information Systems Security Professionals, Field Counterintelligence Specialists, and Field Office Chiefs. IS Reps were the most highly rated field personnel, but the results indicate this could be attributed to the more frequent interactions IS Reps have with their industry counterparts. In general, respondents noted an increase in professionalism and responsiveness across the entire range of field personnel. Respondents did note however, that field personnel could improve their understanding of their company's line of business and spend more time interacting with senior management officials.

Capturing data on individual field office satisfaction allows Field Operations to identify trends or spot problems in specific locations. The field offices that received the lowest ratings this year tended to have a higher turnover rate of personnel than the more highly rated offices. High turnover equated to fewer interactions, uncertainty on the part of FSOs, and even inconsistent application of the National Industrial Security Program Operating Manual (NISPOM). Field offices with highly favorable ratings were perceived as having professional, responsive reps with a thorough understanding of the NISPOM.

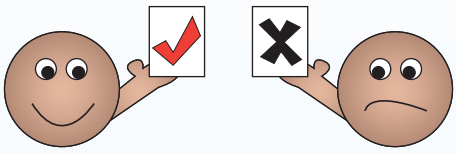
The FSOs responding to the survey offered several suggestions for continued improvement at DSS. At the top of the list was a desire for more consistency in assessments, interpretations of the security rating matrix, and advice. Related to this was a desire from some smaller facilities for a customized approach that would better fit their needs. FSOs recognized that staffing shortages across DSS lead to diminished support and they see a need for more experienced reps with relevant backgrounds. Respondents also asked for as much training, security-related materials, and events as DSS could provide. Finally, respondents asked for even more collaboration and communication.

Based on the responses to this year's survey, the agency is developing an action plan to address FSO suggestions and concerns. For example, the agency will continue to enhance overall communications and ensure that substantive changes to policy are more widely broadcast. As always, DSS will focus on retaining top talent and continuing to build longer-term relationships between DSS and industry. These initiatives will be measured in next year's survey to ensure they are having the desired impact.

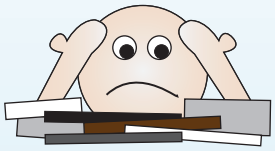
Key Themes of this Year's Results



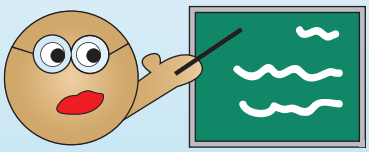
Frequency of interactions
and duration of relationships had a significant impact on customer satisfaction levels.



Dissatisfied participants blamed
inconsistencies between representatives
with respect to interpretation of policy and assessment techniques.

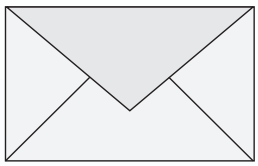


Respondents indicated that DSS field personnel seemed **overburdened**, with limited capacity to meet the needs of industry.



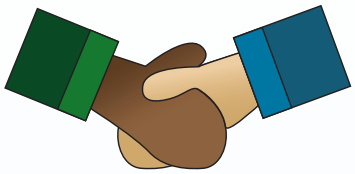
Increased communication and expanded training/education offerings
are key components to improving relationships with industry.

VOICE OF INDUSTRY: RESULTS IN NUMBERS



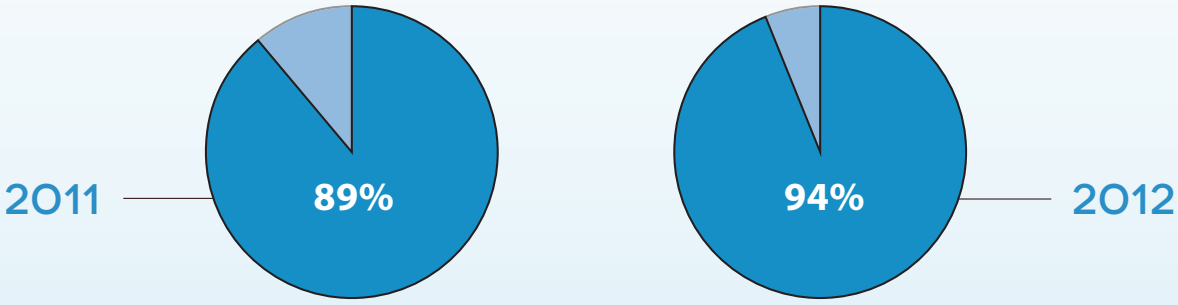
More than
13,000 FSOs
received the survey.

Approximately
10,000 FSOs
responded.

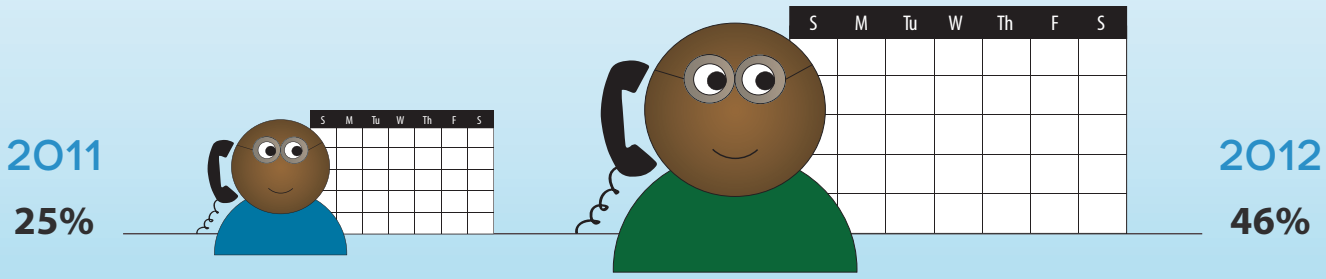


83% of respondents
said they have a true
partnership with DSS.

Overall Level of Satisfaction with DSS



Percent of FSOs that indicated DSS works with them at least monthly



DSS MARKS 40TH ANNIVERSARY

This year marks the 40th anniversary of the Defense Security Service (DSS). And if there is one constant a reader can glean from the agency's history, it is change.

Originally established as the Defense Investigative Service (DIS), the agency has been through multiple reorganizations, staffing and budgeting ups and downs, and one name change. It has added and shed significant missions to the extent that today's DSS no longer accomplishes the same mission it was originally assigned in 1972.

It has moved its headquarters from Washington, D.C., to Alexandria, Va., and finally to Marine Corps Base, Quantico, and opened and closed offices across the country. The workforce has changed from a roughly equal military/civilian mix to an exclusively civilian organization. And it has fielded enterprise-wide information systems that, while cutting edge at the time, have long faded into obsolescence.

In short, the history of DSS largely mirrors the history of the Department of Defense and its shift to consolidation, reliance on information technology and constant pressure to meet new, evolving requirements.

DIS was established as a result of a 1970 Blue Ribbon Defense Panel recommendation for a single, centrally directed DoD personnel security investigative service. Prior to the formation of DIS, each military service conducted its own investigations, and investigators made duplicative visits to the same local agencies to conduct education and local law enforcement checks.

On Dec. 29, 1971, Secretary of Defense Melvin Laird directed that DIS be created as a separate Defense Agency reporting directly to the Secretary of Defense. Since then, the agency has been aligned under the Assistant Secretary of Defense (Comptroller), the DoD General Counsel, the Under Secretary of Defense for Policy, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), and now, the Under Secretary of Defense for Intelligence.

Thus, DIS was established on January 1, 1972. On Feb. 28, 1972, Air Force Brig. Gen. Joseph Cappucci, formerly director of the Air Force Office of Special Investigations (OSI) was appointed Director of DIS. He assumed his duties on April 1, 1972.

The time-phased course of action directed by Secretary Laird stipulated that DIS would assume case control of personnel security investigations (PSI) within DoD on April 1, 1972. From May to October 1972, DIS functioned with a small headquarters staff and relied completely on existing investigative organizations to accomplish its mission. On Oct. 1, 1972, all PSI field investigative resources were transferred from the military services to DIS and investigations were assigned directly to DIS.

The caseload of PSIs at the time of the establishment of DIS was approximately 200,000. A total of 3,000 authorized manpower spaces (of which approximately

TIMELINE: Publications By the Defense Investigative Service in, from left, 1989, 1990, 1992, 1993.

1,750 were military) were transferred from the military services to DIS for the establishment of the PSI mission. By the end of FY84, DSS was an entirely civilian organization.

At the time of its standup, DIS was also assigned responsibility to maintain the Defense Central Index of Investigations (DCII) for the Department. At the time, DCII was maintained on an IBM 360/40 computer located at Fort Holabird, Md. The DCII Master Index was composed of approximately 15 million locator records for investigations conducted by or for DoD investigative agencies and retained by them.

In 1977, DIS was assigned the mission of law enforcement in detecting fraud, waste and abuse in DoD. Unlike other new missions that remained with the agency, this mission was transferred to the DoD Inspector General in 1981 and the Defense Criminal Investigative Service (DCIS) was then formed. At the time, the criminal investigation mission under DIS focused primarily of the theft of government property at facilities of the Defense Logistics Agency (DLA).

A major change in the agency's mission set occurred in 1980 when the Industrial Security Program was transferred from DLA to DIS. The goal was to achieve industrial security coordination among the military services and the Defense Agencies. To implement the Industrial Security mission, DLA transferred 670 personnel spaces while the military services added 88 more. Shortly after the transfer, in September 1980, there were approximately 10,733 facilities in the Defense Industrial Security Program.

The National Industrial Security Program (NISP) was created by Executive Order 12829 in January 1993, and was intended to replace not only the DISP, but the industrial security programs of the Central Intelligence Agency, the Department of Energy, and the Nuclear Regulatory Commission. The National Industrial Security Program Operating Manual (NISPOM) became effective on April 1, 1995, formally implementing the National Industrial Security Program. It was considered the most significant change in the Industrial Security Program in nearly 40 years.

Today, the NISPOM (revised and re-issued on February 28, 2006) serves as the basis for DSS oversight of the program. There are approximately 13,300 facilities cleared under the NISP and the industrial security program forms the foundation of the agency's current mission set.

During the same time, DSS was providing administrative support for the DoD Security Institute (DoDSI) located near Richmond, Va. DoDSI trained DIS personnel security investigators and industrial security representatives and also offered resident and extension courses for U.S. government employees and industry representatives.

In 1983, the Institute trained approximately 3,800 students. In 1997, Defense Reform Initiative #2 directed

that DoDSI, the DoD Polygraph Institute (DoDPI) and the Personnel Security Research Center (PERSEREC) be integrated into DIS. The Defense Reform Initiative also directed a name change for the agency and on November 25, 1997, the Defense Investigative Service was changed to the Defense Security Service, in recognition of the agency's "broader missions and functions."

In 1999, the Defense Security Service Academy was formally established and in 2007, the Director of DSS was named the functional manager for DoD Security Training. In 2011, there were over 200,000 course completions through the Center for Development of Security Excellence.

A counterintelligence office was established at DSS in May of 1993 in response to a recognized need for information of intelligence and counterintelligence value collected by DSS in the performance of its assigned functions. The information was analyzed and referred to agencies and contractors with an official interest in the information.

That need continues today and the agency's CI Directorate continues to develop its analytical capability and deliver high quality products to industry, law enforcement, and investigative agencies.

In February 2005, DoD transferred the personnel security investigations functions performed by DSS to the Office of Personnel Management (OPM). However, DSS retained the mission of adjudicating the eligibility of contractor personnel for access to classified information at the Defense Industrial Security Clearance Office (DISCO).

DSS also retained the function, on behalf of DoD, to oversee the OPM

THE ORIGINAL:
Air Force Brig. Gen. Joseph Cappucci

DIRECTORS OF THE DEFENSE SECURITY SERVICE

Air Force Brig. Gen. Joseph Cappucci, 1971-1976

Bernard J. O'Donnell, 1976 -1981

Thomas J. O'Brien, 1981-1988

John F. Donnelly, 1988 -1996

Margaret R. Munson, 1996 -1998

Steven T. Schanzer, 1998 -1999

Charles J. Cunningham Jr., 1999 - 2002

William Curtis, 2002 - 2004

Heather Anderson, 2004 - 2005

Janice Haith, 2005 - 2006

Kathleen M. Watson, 2006 - 2010

Stanley L. Sims, 2010 - Present

RE-SEALED:
The DSS seal and the DIS seal (right).

SYMBOLISM BEHIND THE SEAL OF THE DEFENSE SECURITY SERVICE

The three divisions of the shield refer to the three basic requirements of all investigations: patient inquiry, observation, and careful examination of the facts.

The eagle, adopted from that used in the seal of the Department of Defense (DoD), alludes to keenness of vision, strength, and tenacity that symbolizes DSS.

The three arrows, also adopted from the DoD seal, refer to the Armed Services, comprising the military components of DSS. In crossing over and protectively covering the Pentagon, these arrows represent the DoD-wide aspects of the DSS mission.

The color dark blue, the national color, represents the United States, and the color light blue represents DoD, the shade of blue being used by the Defense Department. The pattern indicates the integral unity of the United States, DoD, and DSS. The color gold (or yellow) is symbolic of zeal and achievement.

On a white disc within a border of blue with gold outer rim is the shield of DSS in full color blazoned above a wreath of laurel and olive proper (as depicted on the DoD seal).

Inscribed at top of the white disc is "Defense Security Service" and in the base, in smaller letters, is "United States of America," all letters gold.

The laurel and olives symbolize merit and peace; the color white signifies "deeds worthy of remembrance."

billing and financial reconciliation process for PSIs for the entire Department. The transfer included approximately 1,850 personnel and transformed DSS.

Until the transfer of the mission, DSS was synonymous with PSI investigations, and investigative timelines and backlogs were the focus of multiple studies, reports, and Congressional hearings.

The PSI mission had been the primary focus for the agency and largely overshadowed all other missions.

Since the transfer, DSS has reinvigorated its focus on industrial security, security education and counterintelligence and instead, began to be known for its partnership with industry.

It is a process that continues to evolve, but one that the current agency embraces as it looks forward to the next 40 years.

26 FACILITIES ACHIEVE HIGHEST SECURITY RECOGNITION

By Laura Aghdam
NISP Team Action Officer

On June 13, 2012, the Defense Security Service presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 26 cleared contractor facilities. The winning facilities represent the "best of the best," and their security programs stand as models for others to emulate.

These 26 facilities represent less than 1 percent of the over 13,300 cleared contractors in the National Industrial Security Program (NISP). Among the 26 winners were two category "AA" facilities, which are among the largest in the NISP, demonstrating that even the most complex security programs have the ability to attain this honor.

Equally impressive was Lockheed Martin Corporation's six winning facilities, showing that a culture of security and corporate support can and does make a difference.

In order to win a James S. Cogswell Award, facilities must demonstrate excellence in all areas of their industrial security programs. Winners must also receive two consecutive "Superior" ratings, exceeding the baseline requirements of the National Industrial Security Program Operating Manual (NISPOM).

Furthermore, a Cogswell winner provides leadership to other cleared facilities and actively participates in security awareness groups, such as local Industrial Security Awareness Councils and NCMS chapters, whose objectives are to foster communication and enhance security practices across the security community.

Each year, NCMS hosts the Cogswell Award presentations during its annual training conference, where DSS also provides training to industry on a wide variety of subjects ranging from the new DSS security rating matrix to counterintelligence reporting. This year the conference took place in Orlando, Fla., and the awards were presented by DSS Director Stan Sims.

The James S. Cogswell award was originally established in 1966 and was named in honor of the late Air Force Col. James S. Cogswell, the first chief of a unified industrial security program within the Department of Defense.

In creating this joint program, Cogswell focused on the partnership between government and industry in protecting classified information. The Cogswell Award rewards those contractors who demonstrate superior support of this partnership and common goal.

Please join DSS in congratulating the 2012 James S. Cogswell Award winners listed at right!

Alion Science and Technology Corporation
Pascagoula, Miss.

ARINC Engineering Services, LLC
Annapolis, Md.

BAE Systems, Inc.
Arlington, Va.

Ball Aerospace & Technologies Corp.
Albuquerque, N.M.

DCS Corporation
Alexandria, Va.

Electric Boat Corporation
North Kingstown, R.I.

Espey Mfg. & Electronics Corp.
Saratoga Springs, N.Y.

General Dynamics Armament and Technical Products-Camden Operations
Hampton, Ark.

L-3 Communications Sonoma EO, Inc.
Santa Rosa, Calif.

L-3 Communications Corporation ComCept Division
Rockwall, Texas

Lockheed Martin Corporation – Corporate Headquarters
Bethesda, Md.

Lockheed Martin Corporation – Global Training & Logistics
Orlando, Fla.

Lockheed Martin Corporation – Mission Systems & Sensors
Manassas, Va.

Lockheed Martin Corporation – Mission Systems & Sensors
Syracuse, N.Y.

Lockheed Martin Corporation – Mission Systems & Sensors
Middletown, R.I.

Lockheed Martin Services, Inc. – IS&GS-Defense
Colorado Springs, Colo.

Northrop Grumman Corporation, Aerospace Systems
Melbourne, Fla.

Raytheon Company
Garland, Texas

Raytheon Technical Services Company LLC
Indianapolis, Ind.

Schafer Corporation
Albuquerque, N.M.

Sierra Nevada Corporation
Sparks, Nev.

SRI International
Menlo Park, Calif.

STG, Inc.
Reston, Va.

System Planning Corporation
Lexington Park, Md.

TSM Corporation
Bartlett, Tenn.

University of Central Florida
Orlando, Fla.

NEW FOCI COLLOCATION REVIEW PROCESS

By Brian Reissaus
Industrial Policy and Programs

Based on feedback from the Foreign Ownership, Control or Influence (FOCI) community, in April 2012, the Defense Security Service (DSS) established a new process for reviewing potential FOCI facility collocations. FOCI collocation occurs when a FOCI company's proximity to an affiliate, as defined in the FOCI mitigation agreement, reasonably inhibits their ability to comply with the agreement. FOCI collocation is not authorized, and DSS will determine when a FOCI company located in close proximity to an affiliate is considered collocated.

The new process provides more transparency to industry on concerns that DSS associates with FOCI collocations and improves consistency in the assessment of potential collocations. To help industry acclimate to the new process, DSS developed the Facilities Location Plan (FLP) template which establishes a uniform method for FOCI companies to provide the necessary information to DSS for review.

The template was developed as a tool for FOCI companies to demonstrate the effective mitigation of all risks associated with being located in proximity to an affiliate. It is incumbent upon the FOCI company to submit the FLP to DSS. In completing the FLP, FOCI companies and their respective Government Security Committees (GSC), will outline the proposed/established mitigation measures for these risks. Detailed completion of the FLP template will ultimately facilitate DSS review of potential FOCI collocations and help ensure the GSC is able to maintain effective and continuous oversight.

If the FLP proves being located in proximity to an affiliate does not degrade the ability to comply with all terms of the FOCI mitigation agreement, DSS will approve the FLP and determine that FOCI collocation is not present contingent upon adherence to the approved FLP and FOCI mitigation agreement.

In addition to the FLP template, the most significant change to the process was redefining FOCI collocation. The new definition moves away from specific scenarios, and focuses on compliance with the FOCI mitigation agreement.

Included in the DSS review is a site visit to determine the feasibility and effectiveness of the FLP. This review will assess the FLP to ensure risk factors such as possession of classified materials, onsite key management personnel from the ultimate foreign parent and FOCI company, and potential non-compliance with the terms of the FOCI mitigation agreement, are effectively mitigated.

All FLPs will be reviewed locally by the servicing DSS Field Office and ultimately by the FOCI Operations Division before a final determination is made. Additionally, DSS will review the implementation of an approved FLP as a part of the annual security vulnerability assessment to ensure the FLP is effective.

Companies with previously approved collocations plans are not required to submit new FLPs. However, any substantive changes made to existing collocation plans will require resubmission for review and approval. For more information about the new FOCI collocation review process and a copy of the FLP template, visit the DSS website at http://www.dss.mil/isp/foci/foci_collocation.html.

SECURITY CLEARANCE REQUESTS REJECTED FOR LACK OF INFORMATION

By Phu Nguyen
Defense Industrial Security Clearance Office

Incomplete information is the most common reason why security clearance application packages are rejected by either the Defense Industrial Security Clearance Office (DISCO) or the Office of Personnel Management (OPM).

Incomplete information could be the subject failing to indicate the company submitting the investigation request is their current employer; missing fingerprint cards; subject failing to provide identifying information for relatives born abroad; or subject failing to provide Selective Service registration information or legal exemption.

To expedite the security clearance process, applicants and security officers should ensure all forms are completed and contain accurate information.

They should also familiarize themselves with how a properly rolled set of fingerprints should look, and when possible, list references located in the United States who can verify overseas activities.

Turn the page to see charts identifying the most common reasons investigations are rejected by DISCO and OPM and how to correct them.

THE FOLLOWING ACCOUNT FOR **92%** OF INVESTIGATION REQUESTS REJECTED BY **DISCO:**

1	**Missing employment information**	List all employment; include the company submitting the clearance request as current employer. Applicant should list all full-time work, paid or unpaid, consulting/contracting work, all military service duty locations, temporary military duty locations (TDY) over 90 days, self-employment, other paid work, and all periods of unemployment.
2	**Missing information on relatives born abroad (U.S. citizen/ national)**	Applicant must provide information for relatives required to be listed, living or deceased, including full name, date of birth, place of birth (city, state or country), present residence and citizenship. Do not provide information on relatives NOT listed in these categories: Mother, father, stepmother, stepfather, foster parent, child, stepchild, brother, sister, stepbrother, stepsister, half-brother, half-sister, father-in-law, mother-in-law, and guardian. For relatives who are United States citizens or Nationals, and who were born outside the United States, information regarding proof of citizenship, including document identification numbers, from any or all of the following documents, must be provided: U.S. passport (if the subject has been issued a passport); "Consular Report of Birth Abroad of a Citizen of the United States of America" (FS-240); Citizenship Certificate.
3	**Missing Selective Service registration information**	A male applicant born after December 31, 1959, who has not registered for Selective Service, must fully explain the reasons for not having registered, with reference to any applicable legal exemption(s). Persons can verify their Selective Service registration and obtain their registration information online from the Selective Service System at the web site http://www.sss.gov or telephonically at 1-847-688-6888.
4	**Incomplete information about debt / bankruptcy**	Disclose all financial obligations which are delinquent, and all information pertaining to bankruptcy. Include dates, amounts, account numbers, and name of the organization to which debt is/was owed.
5	**Missing social security number for adult co-habitant**	Provide complete information for each field. If cohabitant is a U.S. citizen born outside the United States, provide complete proof of citizenship information, including document identification numbers.
6	**Missing information on current spouse**	Provide complete information for each field. If spouse is a U.S. citizen born outside the United States, provide complete proof of citizenship information, including document identification numbers.
7	**Missing education reference information**	Provide complete name and address of the school and a person who has knowledge of the applicant. If the most recent degree falls outside the scope of the investigation (7 or 10 years), provide information regardless of how long ago the degree was obtained.
8	**Missing employment reference information**	If unemployed or self-employed, applicant must identify and provide contact information for a person who can verify the unemployment or self-employment (may use spouse, parents or siblings as the verifying reference).
9	**Missing employment record information**	Provide additional employment details such as being fired from a job; quitting after being told you would be fired; leaving a job by mutual agreement of unsatisfactory performance, and/or receiving written warnings; or being officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as a violation of security policy.
10	**Missing personal reference information**	Applicant must provide names of at least three individuals and include complete U.S. addresses and phone numbers. These are not to be relatives, spouses, former spouses, or anyone listed anywhere else on this form. Applicant will also need to include a work or home address, as well as zip code and current phone number(s).

THE FOLLOWING ACCOUNT FOR **98%** OF INVESTIGATION REQUESTS REJECTED BY **OPM:**

1	**Fingerprint cards not submitted within the required timeframe**	Fingerprint cards must be provided to OPM within 14 days of approval by DISCO. More details on when and how to submit fingerprint cards is available on the DSS website: (http://www.dss.mil/disco/indus_disco_process_applicant.html#Fingerprint Cards).
2	**Illegible or missing information on release forms**	Provide complete information for each field and ensure there are no stray marks on the forms, and ensure the top, bottom and sides of each document are present after scanning attachments. Type or legibly print the name, SSN, address and dates. Use the date format mm/dd/yyyy.
3	**Forms do not meet date requirements**	Use the date format mm/dd/yyyy. The forms cannot be older than 120 days.
4	**Erroneous place of birth information**	Provide city, county and state; or country, if born outside of the U.S. Place of birth must be accurate and consistent with other forms.
5	**Erroneous date of birth information**	Date of birth must be accurate and consistent with other forms. Use the date format mm/dd/yyyy.
6	**Request ID number on e-QIP does not match the number on the certification and/or release(s)**	Pages printed from e-QIP contain the request ID of the questionnaire completed by the applicant, and must match the investigation request ID being submitted to OPM. The request ID number cannot be hand written.
7	**Certification/release forms not submitted**	The personnel security investigation cannot proceed without a signed and current release form. Scan and attach the forms in JPAS. The Fair Credit Reporting Disclosure and Authorization form is required.
8	**Missing references (character, residential, employment, or educational)**	Applicant must provide names of at least three individuals and include complete U.S. addresses and phone numbers. These are not to be relatives, spouses, former spouses, or anyone listed anywhere else on this form. Applicant will also need to include a work or home address, as well as zip code and current phone number(s). If unemployed or self-employed, applicant must identify and provide contact information for a person who can verify the unemployment or self-employment (may use spouse, parents or siblings as the verifying reference).
9	**Incorrect social security number**	The SSN must be entered accurately and must be consistent with other submitted forms.
10	**Missing employment information**	List all employment; include the company submitting the clearance request as current employer. Applicant should list all full-time work, paid or unpaid, consulting/contracting work, all military service duty locations, temporary military duty locations (TDY) over 90 days, self-employment, other paid work, and all periods of unemployment.

NISP COMPLIANCE

In December 2010, the Defense Industrial Security Clearance Office (DISCO) began an initiative to review Joint Personnel Adjudication System (JPAS) records for overdue periodic reinvestigations (PR) of cleared contractor personnel.

DETAILS

In September 2011, DISCO identified two cleared contractors with overdue PRs. The President/Facility Security Officer (Subject 1), cleared at the Top Secret (TS) level, was two years overdue for his PR, and his son (Subject 2), also cleared at the Top Secret level, was nine years overdue for his PR.

However, DISCO was unaware these individuals were key management personnel (KMP) as no identifier existed in JPAS. The company possessed a Top Secret Facility Clearance (FCL) and was granted Secret safeguarding by another cognizant security agency (CSA).

DISCO sent a JPAS request to the facility for an e-QIP submission for both KMPs but received no response. As a result, in October 2011, DISCO entered a Loss of Jurisdiction (LOJ) in JPAS, suspending both KMPs' access to classified information. Soon after, while preparing for the facility's annual security assessment, the Industrial Security Representative assigned to the facility discovered the KMPs eligibility reflected as LOJ in JPAS.

DSS scheduled a meeting with the KMPs to discuss:

- What the LOJs meant in terms of their roles and responsibilities as KMPs (no access to classified information, submitting e-QIPs, and need to appoint an interim FSO);
- The need for the company to submit and follow a plan of action to update the overdue PRs; and
- Establishing a JPAS account for an eligible and authorized person. Subject 1 had been locked out of his JPAS account due to inactivity. As a result, the facility was unable to receive/review JPAS messages sent by DISCO or submit e-QIPs.

During the meeting, both KMPs refused to appoint a new JPAS account manager; refused to take action to deny themselves access to classified information while in LOJ status; and refused DSS access to the facility security container to inventory the contents.

The KMPs took exception to the LOJ status, contending they were notified after the action had been taken.

The KMPs stated "... DSS essentially revoked the Government clearance with the immediate consequence that existing contracts involving the need for clearance had to be instantly terminated." The facility was performing on one classified contract

under DSS cognizance and on one contract under another CSA.

Both KMPs refused to take appropriate actions to become compliant with the National Industrial Security Program. As a result, the company's FCL was invalidated and administratively terminated the following month at Subject 1's request.

LESSONS LEARNED

Between 2006 and September 2010, four separate security assessments noted the overdue PRs and documented them as findings in the Industrial Security Facilities Database (ISFD), but no follow up actions were taken.

- KMP who are overdue periodic reinvestigation are now being identified by DISCO on a monthly basis. Communication with the applicable company is now taking place via JPAS notifications and email/ telephonic contacts to ensure awareness of pending PR submission requests.

When Subject 1 was locked out of his JPAS account due to inactivity, he could not maintain the accuracy of his employees' records in accordance with DoD 5220.22-M, National Industrial Security Program Operating Manual, Section 2-200b.

- DSS is developing an initiative for tracking JPAS account use by last log-in date to identify possible inactivity issues. Accessing JPAS accounts on a regular basis allows the contractor to maintain the accuracy of their employees' access records and monitor JPAS notifications. DSS is actively reviewing this activity as part of our assessment process and we encourage industry to incorporate this component into their contractor self reviews.

There was another complicating factor in this situation. The facility's original Commercial and Government Entity (CAGE) code was issued in 1974; a new CAGE code was issued on October 21, 1998. On November 29, 1999, the facility first came under DSS cognizance and received a Top Secret facility clearance. For reasons unknown, when data was migrated into JPAS in late 2004, the incorrect (original) CAGE code was placed on the facility's profile rather than the second one.

The correct (new) CAGE code was updated in JPAS in February 2009, however discrepancies remained in JPAS.

- This means even if the FSO had not been locked out of his JPAS account, he still would not have received the e-QIP notifications since they were sent to the wrong CAGE code. Since the CAGE code is tied to the Security Management Office code, this discrepancy should have been discovered by the facility.

DSS has implemented a rigorous post assessment process to ensure all vulnerabilities identified during security assessments (to include overdue PRs) are mitigated in a timely manner. DSS will provide companies with a listing of all identified vulnerabilities and request that a written response outlining procedures or policies be put in place to correct the cited vulnerabilities. DSS may also schedule a follow-up visit to the company to validate the effectiveness of the corrective actions taken.

FIRST STUDENTS COMPLETE

COLLEGE, GRADUATE-LEVEL COURSES AT CDSE

The first students enrolled in the new Challenges in Analyzing and Managing Risk course offered at the Center for Development of Security Excellence (CDSE) successfully completed the course in May.

The three students — Rocky McCollum and Jeff Thoma from the United States Air Force Academy, and Gerald Barb from the Defense Logistics Agency — received strong support from their supervisors and employing activities.

The Challenges in Analyzing and Managing Risk course includes the requirement for each student to complete a semester-long project in which the student uses the Analytical Risk Management model to address a security issue at his or her employing agency.

These recent graduates gathered and analyzed information about the value and criticality of certain assets at their agency, threats to those assets, and vulnerabilities that exist which result in risk to the organization or its mission. They then identified cost-effective countermeasures which could be put in place to reduce the risk to an acceptable level.

During the last week of the course each student presented the project that he or she completed including recommendations for next steps to be taken by the agency. These recommendations may be presented by the students to decision makers at their employing agencies.

Approximately 45 students are participating in other college-level and graduate-level classes at the CDSE during the summer semester.

Students participating in these classes typically devote 15 to 20 hours per week to studying during the 16-week semester, including reading, writing, and participating in online discussions with the instructor and other students. The level of effort required to complete the courses is similar to that required to complete a graduate-level course at a university.

Prior to enrolling in one of these courses, it is important for a student and his or her supervisor to reach a common understanding of how much of this study time can be done during duty hours and how much will be done during non-duty hours.

During the first semester in which the courses were offered, a significant number of students dropped out after realizing the amount of time required to complete the course

assignments. Many of those students indicated that they will plan their schedules to allow them to take the classes when they are offered again next year.

Students take these courses for many different reasons. Some said they enrolled in a course because they enjoy the intellectual challenge and interaction with other students. Others indicated that they want to become more competitive when they apply for new jobs or promotions.

When asked why he is taking the Understanding Adversaries and Threats to the United States course, Scott Hill, instructor at CDSE replied, "I'm taking the class because as a leader within DoD it is imperative that I have a thorough understanding of the emerging threats and challenges security professionals face. The fact that CDSE is now offering free semester-long collegiate-level classes now makes my growth as a future leader very attainable."

"THE FACT THAT CDSE IS NOW OFFERING FREE SEMESTER-LONG COLLEGIATE-LEVEL CLASSES NOW MAKES **MY GROWTH AS A FUTURE LEADER** VERY ATTAINABLE."

Jeffrey Cooper, an Air Force employee who is currently taking the Challenges in Analyzing and Managing Risk course, says, "I plan to leverage this course as a CAP Stone course for the 'Palace Acquired Fellowship' program."

Most students enrolled in this new curriculum hold a SPēD Professional Certification, maintenance of which requires completion of professional development units (PDUs). A student can earn 35 PDUs for completing a course in this curriculum. The courses also help to prepare security professionals for the higher-level SPēD Security Program Integration Professional Certification and Security Enterprise Professional Certification.

CDSE introduced this new curriculum of advanced courses to meet the professional development needs of DoD security professionals. Seven of the courses in this curriculum made their debut in FY12. They are:

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

DSS CDSE offers these courses to United States military members and DoD employees without charging any tuition or fees. Students or their employing agencies must obtain textbooks as required by each course. Most of the courses are presented online, using a collaborative learning environment, allowing students to complete the courses without the cost or inconvenience of travel.

Students who are working toward earning a Bachelor's or Master's degree may request the college or university they are enrolled in award transfer credit for CDSE courses they have completed. Courses in this curriculum are designed to be equivalent to upper-division undergraduate or graduate-level courses that would be offered by a university.

Each course will be reviewed by the American Council on Education (ACE) for CREDIT recommendations. Information about the ACE College Credit Recommendation Service can be found at this web site: www.acenet.edu. CDSE courses that have been reviewed by and have received recommendations from ACE are listed at: http://www2.acenet.edu/credit/?fuseaction=browse.getOrganizationDetail&FICE=1007408. More details about the CDSE Security Education program, including course descriptions, dates, prerequisites, and enrollment information, is available at http://www.dss.mil/education/index.html.

DSS OUTFITS DATA CENTER WEST

New information technology setup ensures system redundancy in case of emergency

DSS achieved a major milestone in June regarding its information technology (IT) environment with the outfitting of its Data Center West in Monterrey, Calif. The enhanced data center completes a promise made to DSS Director Stan Sims to upgrade DSS to the latest in IT infrastructure and to provide the best IT service and technology for DSS.

After a year of planning and recent deployment, DSS recently installed major hardware and software components that will allow the agency to closely mirror its IT operations at Quantico, Va.

The Data Center West IT deployment is just one phase that will enable DSS to have enhanced email/Blackberry/file and database capabilities including continuity of operations from redundant systems featuring immediate (or hot) failover capability. In other words, should the data center located in the Russell-Knox Building at Quantico, Va., suffer a power outage, or other system failure, the backup systems at the Data Center West would be called into action.

This failover would ensure the agency's field locations would still have access to agency systems allowing them to continue to work. Likewise, Headquarters personnel located at RKB would have access to email and other systems from alternate work locations during such an event.

The second phase of Data Center West integrated the Industrial Security Facilities Database (ISFD) and maintenance of the DSS public website into the new architecture and also took place this summer.

The third and final phase will add redundancy to mission critical systems that are getting ready to come on line such as the identify Management System and ODAA Business Management System. DSS will also have the ability ensure failover capabilities are in place for systems such as the Security Training, Education and Professionalization Portal (STEPP).

This project had a tight schedule and was completed within nine months to ensure smooth operations in support of the DSS mission. The team was able to meet the timeline and under cost.

BY THE NUMBERS

So, what does it take to design/build/move/install a robust DSS alternate data center?

- $2.2 million in equipment
- Five months of collaboration/planning
- Three months of building servers, software installations, validation, verification, and securing the IT system environment
- 220 megabytes of document development that includes information assurance, configuration, and design
- Three days and five people to un-rack/pack/palletize and move the equipment to the RKB loading dock.
- Four days of racking, installing, testing, and securing equipment

MANUAL LABOR: The OCIO team packed, unpacked, installed, tested, and ensured all was running at Data Center West. From left, Robert Riggle, Kang Kim, Eric Corbin, Jeff Arnold, Frank Sandau, Jerry Ruby, Henry Swietanski, Luis Garcia. Other OCIO team members who supported this project but are not shown include: Mark Failer, John J. Long, Ali Mohammed, Barbara Jackson, Sherry Harrington, and Leslie Summers.

NORTHERN REGION *growing* FUTURE LEADERS

To "grow" better leaders, Mike Halter, Regional Director, and Cheryl Matthew, Regional Operations Manager, Northern Region, created the Leadership Development Program (LDP) to provide employees with opportunities to develop their leadership skills and prepare themselves to compete for and assume positions of increased responsibility within DSS.

The program was started as a pilot in the Northern Region and was intended for employees who aspire to fill leadership positions at some point in their DSS careers, with an emphasis on developing the skills needed to serve as a field office chief. Throughout the program, the employees are mentored by field office chiefs, and goals are set and reviewed each month to ensure each participant achieves a level of knowledge and the ability to successfully perform in a leadership position.

"The intent of the LDP is to provide opportunities for our team to better understand challenges and expectations of field office leadership," said Halter. "Also key to the program is enhancing communications and understanding not only between different field elements but across agency directorates."

Each program participant travels to the Northern Region office, where they meet with the Regional Director and staff, as well as to another field office outside of the Northern Region to see the industrial security mission being managed and executed in a different manner. The program also includes a two-week rotation at DSS Headquarters where employees work with various offices in Industrial Security Field Operations and Industrial Policy and Programs to increase their understanding of these functional areas.

"Having each participant work directly with the offices that support them in the field will expand their knowledge and appreciation for the work being done," said Sarah Laylo, NISP Team Chief. "The visits also include a meeting with senior leaders from Industrial Security Field Operations, Industrial Policy and Programs, and the Counterintelligence directorates, where each participant discusses his/her goals and outlook for the future."

"I found my visit to DSS headquarters to be both educational and beneficial," said Matthew Rennie, Senior Industrial Security Representative from the Detroit Field Office. "Headquarters is much like the field, in that they are managing a maximum workload with minimal staff. Each area is working to support the field by streamlining our processes and providing us tools to help us manage our responsibilities."

Sal Urbano, Industrial Security Representative, St. Louis Field Office, recently completed his headquarters rotation and had this to say about the experience, "It gave me a different perspective of my understanding on the relevance of the work the field is completing in concert with the metrics compiled every month by the region. I understood the metrics but seeing what and how they play such keys roles during Field Operations staff meetings was an eye opener. It was great to see how they really do focus on the field to ensure we have everything we need and where the shortfalls are."

He added that while at Headquarters, he had the opportunity to meet with and discuss 10 different disciplines within DSS. "I was able to see what their role was in DSS and how they help complete the circle. It also gave me the opportunity to walk a couple steps in their shoes to see if it was something I may be interested in the future," Urbano added. "There were some disciplines that I enjoyed more than others. I think the LDP is something that everyone should want to participate in to develop a broader picture and scope of understanding of the role each and everyone plays in the agency."

According to Richard Lawhorn, Director, Industrial Security Field Operations, while still in its early stages of development, the program is working as intended. "It's providing participants with a good overview of the Headquarters to improve communication and understanding across Field Operations." Lawhorn added that the plan is to expand the program in the near future to the other regions with the Western Region scheduled to come on board later this summer.

Editor's note: DSS is developing a Leadership Development Program, which will be available to all employees in early FY13. This new program will incorporate the lessons learned from this Northern Region initiative but also provide expanded opportunities for formal leadership development and training opportunities. Initiatives from individual offices or regions such as this, will continue to be encouraged and will complement and augment the agency-wide program.

DSS PROVIDES KEY SUPPORT

TO NEW EXPORT ENFORCEMENT CENTER

By Matthew Guy
DSS Counterintelligence

In May, DSS Director Stan Sims attended a ribbon cutting ceremony to mark the opening of the Export Enforcement Coordination Center (E2C2).

Established by the President under Executive Order 13558, the E2C2 is responsible for enhanced information sharing and coordination between law enforcement and intelligence officials regarding possible violations of U.S. export controls laws.

"I am excited for DSS to be recognized as one of the key participants of this national-level operation," said Sims. "This is another example of other federal agencies beginning to recognize the value that DSS brings to the security, intelligence, counterintelligence, and law enforcement communities."

The DSS Counterintelligence Directorate provides a liaison officer (LNO) to E2C2 to ensure that DSS suspicious contact reports related to violations of U.S. export control laws involving cleared industry are reviewed by participating agencies.

In addition, the LNO responds to inquiries submitted by the investigative agencies. This routinely involves answering questions about facility and personnel clearances, identifying which technologies may be at risk, and coordinating communication between DSS field personnel, facility security officers, and federal law enforcement officials.

The E2C2 is administered by the Department of Homeland Security (DHS) with a leadership team comprised of officials from DHS, the Federal Bureau of Investigation, and the Department of Commerce.

Other E2C2 partner agencies include the Office of the Director of National Intelligence, and the departments of Justice, State, Treasury, Defense and Energy. There is also representation from the Commerce Department's Bureau of Industry and Security, U.S. Customs and Border Protection, Defense Criminal Investigative Service, and the National Nuclear Security Administration.

The standup of the E2C2 represents a step forward in changing the way the Executive Branch does business by implementing a more fully coordinated and harmonized approach that facilitates secure trade.

Such an approach better protects military critical technologies from being transferred to countries or entities of national security and proliferation concern. It also strengthens the cleared U.S. industrial base by helping U.S. exporters to be more competitive and reliable suppliers. These steps are improving how the U.S. government utilizes its existing resources to ensure that the export control system meets national security and foreign policy objectives.

During his visit to the E2C2 facility, Sims received a private tour of the center from James Dinkins, executive associate director of Homeland Security Investigations, alongside David Aguilar, acting commissioner, U.S. Customs and Border Protection.

"During our time together, I had the opportunity to discuss the DSS mission," said Sims. "It was clear that these senior government officials both had an awareness and appreciation for the value that DSS brings to E2C2 as a result of our access to industry."

E2C2 Director Craig Healy echoed that sentiment during a visit to DSS last year to brief DSS employees on the results of a significant investigation, where he praised the work of DSS. He noted that his relationship with DSS goes back to his days as a field agent, where he relied heavily on the industrial security knowledge and access to industry provided by DSS representatives.

Last year, Immigration and Customs Enforcement (ICE) and the Department of Commerce opened more than 100 law enforcement investigations for violations of U.S. export control laws as a result of DSS Counterintelligence (CI) referrals. For Fiscal Year 2012, the federal law enforcement and intelligence communities are on track to open more than 500 investigations or operations based on DSS CI referrals.

These referrals run the gamut of criminal violations or illegal intelligence activity related to espionage, fraud, export control violations, and illegal disclosures of U.S. classified information, taking place within or directed against the cleared industrial base.

"While we lack federal law enforcement authority, our small agency serves as a force multiplier for the much larger agencies that do," said Sims. "Our relationship with cleared industry provides significant operational and investigative advantages to law enforcement and the other federal communities we support."

CENTER TOUR: DSS Director Stan Sims (left) received a tour of the Export Enforcement Coordination Center from James Dinkins, executive associate director of Homeland Security Investigations for U.S. Immigration and Customs Enforcement.

EXECUTIVE ORDER 13558

assigns the following functions to the Export Enforcement Coordination Center:

Serve as the primary forum within the federal government for executive departments and agencies to coordinate and enhance their export control enforcement efforts. The center will also identify and resolve conflicts that have not been otherwise resolved in criminal and administrative investigations and actions involving violations of U.S. export control.

Serve as a conduit between federal law enforcement agencies and the U.S. intelligence community for the exchange of information related to potential U.S. export control violations.

Serve as the primary point of contact between enforcement authorities and agencies engaged in export licensing.

Coordinate law enforcement public outreach activities related to U.S. export controls.

Establish government-wide statistical tracking capabilities for U.S. criminal and administrative export control enforcement activities. This will be conducted by the Department of Homeland Security with information provided by and shared with all relevant departments and agencies participating in the Export Enforcement Coordination Center.

TRADING PLACES

It was proposed that Regional Directors trade places around the country for two weeks. The rotation would allow the directors to experience and practice their leadership skills in different operating environments.

DSS Field Operations is divided into four geographic regions to better manage the agency's oversight mission and ensure personnel are located in the areas with the highest concentration of cleared facilities. While Field Operations tries to equalize the workload across the regions, each region has its own unique set of facilities and with it, unique challenges.

For instance, the Capital Region is the smallest region geographically, but has the most cleared facilities (approximately 4,325). The Northern Region, on the other hand, stretches from Maine to Detroit, Mich., but has approximately 2,626 cleared facilities. And the Southern (3,600 facilities) and Western (2,700 facilities) Regions have some of the largest manufacturing facilities in the National Industrial Security Program.

Recognizing the regional diversity, Richard Lawhorn, Director, Field Operations, asked the Regional Directors (RDs) to develop a plan for a rotation — in effect have the RDs trade places for two weeks. The rotation would allow the RDs to experience and practice their leadership skills in different operating environments.

The first such rotation occurred in May with Mike Halter, Northern RD, spending two weeks in San Diego, while Karl Hellmann, Western RD, reported to Boston.

"Although we generally do things in the same manner across regions, we all have some unique challenges," said Halter. "This is not a program where we simply sat in each other's chair and went home after two weeks. Rather, we performed all aspects of an RD and assumed all the responsibilities of the position."

Hellmann added, "The main idea is to develop consistency from region to region. We want to identify best practices and develop a more efficient, consistent approach to leading our regions."

During the rotation, both kept daily journals and shared weekly updates with Lawhorn and other Field Operations leaders. The also provided a full assessment to the leadership team at the conclusion of the rotation.

After two weeks on the West Coast, Halter noted, "Not surprisingly, I found our processes are consistent in both the Northern and Western Regions. Our workforce has the same levels of training, dedication, and professionalism, while leadership is focused on agency priorities."

He added that he would continue to recommend cross-regional support opportunities "to provide our Industrial Security Representatives and Information Systems Security Professionals exposure and experience working in different operating environments throughout the country."

Of his experience, Hellmann said, "This rotation provided an opportunity to see firsthand how processes in other regions are implemented. It also allowed me to develop better working relationships throughout the field that will have a positive effect on DSS."

Lawhorn added, "I was pleased with the rotation. It was a bit of an experiment, but I believe both Mr. Halter and Mr. Hellmann gained from the experience and I also believe the both regions benefitted as a number of best practices were identified. I plan to continue the RD rotation process with the Capital and Southern Regions next, and we will look to expand the program to Field Office Chiefs, Regional Designated Approving Authorities and senior ISFO Headquarters staff in the coming months."

MEMORIAL DAY CEREMONY RECOGNIZES THE "COST OF FREEDOM"

"From the American Revolutionary War to present-day operations in Afghanistan, more than a million men and women have died in service to our country. Each Memorial Day, the nation pauses to remember them, and they are the reason we have come together today," said Stan Sims, DSS Director, at a Memorial Day wreath-laying ceremony held at the Russell-Knox Building, Quantico, Va., on May 24, 2012.

"We are also honoring the memories of the 168 men, women, and children — among them five DSS employees — who died in the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995. Their service to the nation — and the ultimate price they paid for that service — are in our hearts and memories forever," Sims added.

The ceremony was the brain child of Selena Hutchinson, Office of the Designated Approving Authority and Air Force Veteran. Hutchinson began an annual Memorial Day wreath-laying tradition while she worked at the Federal Bureau of Investigation and wanted to start a similar tradition at DSS.

She organized a grass-roots group of DSS veterans who served as ushers, organized a reception, set up chairs and podium and contributed food and funds.

In establishing the annual event, Hutchinson also enlisted the support of Sims (an Army veteran) and Barry Sterling, Chief Financial Officer and Director, Business Enterprise (Air Force veteran) who sponsored the ceremony. Sterling provided the Invocation and Benediction for the event and set the stage in his opening prayer by saying, "May we never fail to remember the incredible cost of the freedom which we enjoy."

In her introductory remarks, Hutchinson emphasized that Memorial Day "is not about beaches, it's not about picnics, and it's not about auto races". She said that it is, instead, an opportunity to remember those who have lost their lives defending freedom. "Their sacrifice was important. Their sacrifice was noble. And their sacrifice was permanent," Hutchinson said.

"Everyone who wears the uniform knows that he or she may be called upon to fight and, if necessary, make the ultimate sacrifice for the most precious and costly of gifts: freedom," said Sims during his keynote address. "I want to be clear: freedom is a gift. It has been paid for by those who gave everything to defend it, and we stand here today on the shoulders of those who answered the call."

Sims also acknowledged and thanked the 16 Wounded Warrior veterans serving as part of the DSS family; some of whom were present for the occasion.

As DSS employees, veterans and building occupants looked on, Sims and Hutchinson placed a wreath at the base of the DSS flag pole while Marine Corporal Kenneth Harper, a bugler from the Quantico Band, sounded Taps.

PHOTOS: Marine Corporal Kenneth Harper, a bugler from Marine Corps Base Quantico Band, sounds Taps. DSS Director Stan Sims and Selena Hutchinson, ISFO Office of the Designated Approving Authority and event coordinator, lay a wreath at the ceremony.

DSS HOTLINE AVAILABLE FOR REPORTING MATTERS OF NATIONAL SECURITY SIGNIFICANCE

The Inspector General (IG) of the Defense Security Service maintains a hotline to provide an unconstrained avenue for government and contractor employees to report, without fear of reprisal, known or suspected instances of serious security irregularities and infractions concerning contracts, programs, or projects. This is in addition to the other federal agency hotlines cited in paragraph 1-207 of the National Industrial Security Program Operating Manual.

The DSS IG Hotline does not supplant contractor responsibility to facilitate reporting and timely investigation of security matters concerning its operations or personnel, and contractor personnel are encouraged to furnish information through established company channels.

However, the DSS IG Hotline may be used as an alternate means to report this type of information when considered prudent or necessary. Contractors shall inform all employees that the hotline may be used, if necessary, for reporting matters of national security significance.

The Defense Security Service IG is organizationally structured under the Office of the Director, DSS. The IG promotes the economy, efficiency, and integrity of DSS personnel, programs, and operations in support of DSS' National Industrial Security Program mission.

To contact the DSS IG Hotline:

Defense Security Service
Inspector General Hotline
27130 Telegraph Road
Quantico, VA 22134

Toll Free: 855-865-1508
Commercial: 571-305-6660
Inspector.general@dss.mil

EEO OFFICE PROGRAMS HIGHLIGHT DIVERSITY

This year, the DSS Equal Employment Opportunity Office hosted several Special Emphasis events within the Russell-Knox Building for Headquarters employees: (Above) A Jamaican Folklore Quartet sings, while Mario Medina, DSS Office of the Chief Information Officer, accompanies with the conga, during a Caribbean American Heritage event. (Below) A member of the Asian American Arts Center Korean Drum and Dance Group performs a fan dance in recognition of Asian Pacific American Heritage Month.

In addition to these events, the agency marked Black History Month with guest speaker Hari Jones from the African-American Civil War Museum, as well as weekly movie days which highlighted African American contributions in every war since the American Revolution. Thereafter, an observance for Holocaust Remembrance Week featured videos chronicling people whose actions during World War II saved lives.

A successful Special Emphasis Program organizes and facilitates activities to celebrate a respective special emphasis month or time of recognition. Other events may focus on educating employees about career advancement techniques or cultural differences to promote a harmonious and inclusive work place.

Observances are conducted to recognize the continuous achievements of all Americans in our culture and to enhance our cross cultural awareness, mutual respect and understanding of our collective human history. The activities support the objective of providing a work place free of discrimination and harassment, and promote a fostering, caring environment.

ODNI RECOGNIZES DSS EMPLOYEES WITH MERITORIOUS UNIT CITATION

In May, Sandy Rausch, Resource Advisor for the Counterintelligence Directorate, and Scott Buchanan, Chief, Budget Execution Office, Financial Management Division, received a Meritorious Unit Citation from the Office of the Director of National Intelligence (ODNI) for their work on the National Intelligence Program (NIP) Execution Team.

The NIP Execution Team was recognized for exceptional achievement in helping to define a future state to improve the quality, quantity, and accuracy of NIP financial data.

From October 2010 to August 2011, Rausch and Buchanan represented DSS on the team that also included representatives from other DoD agencies and services throughout the Intelligence Community (IC).

"Being a part of this team allowed us to have input into the intricacies of setting up a new mechanism in the federal funding arena," said Buchanan. "Providing input to those who are building this new mechanism allowed Sandy and I to excel beyond the confines of the agency and the Department. The experience and the knowledge gained through this process was well worth the time."

As a part of the study, ODNI researched the possibility of combining all appropriations under its purview into one Treasury Index, which would provide better transparency and reportability across the IC, and between ODNI and the Office of Management and Budget.

The study also established the initial groundwork for ODNI to communicate with the Office of the Secretary of Defense and other comptrollers on a way forward to appropriately represent all federal agencies.

The proposed process provides ODNI with pivotal accounting data in a near-real-time manner through the use of the Common Government-wide Accounting Classification which establishes a standard financial structure across all agencies that is recognized on a government-wide basis. It also supports the Financial Management Line of Business (FMLoB) vision for standardization, which is one of the President's top management priorities to achieve government-wide cost and quality improvements in financial management.

According to a White House fact sheet on the FY12 Federal Budget, "the 2012 Budget request represents a focused effort for the DNI to introduce greater fiscal discipline with the NIP. Although not subject to the President's freeze on non-security discretionary spending, the DNI has conducted an efficiencies review similar to that of the Department of Defense. The DNI has used many of these identified efficiencies to reduce the growth in spending within the Intelligence Community."

CDSE MAKES SECOND TRIP DOWN UNDER

The Center for Development of Security Excellence (CDSE) delivered the Introduction to Special Access Programs (SAPs) course to 18 Australian citizens in Canberra, Australia, in May. This was the second iteration of the course delivered by CDSE instructors in Australia.

The training was provided to Australian personnel in support of the Joint Strike Fighter (JSF) program, under the Memorandum of Agreement between CDSE and the JSF Program Office. The goal is to provide more cost effective training and establish the bench strength needed to honor approved security commitments for joint United States/Australian programs. The course teaches the application of U.S. doctrine and although it was conducted at the unclassified level, the training was conducted in a SAP-accredited environment, to allow students to gain first-hand experience of being employed in a SAP facility.

Australia has requested the training be done on a biennial basis in the future, and has asked for assistance from CDSE instructors to aid in developing training packages and building a library of doctrine compatible with U.S. government requirements.

Additionally, the Australians expressed an interest in developing a train-the-trainer program for this course.

Alexandria Field Office Builds Their Team

HEAVY LIFTING: From left, Lanie Peckar, Annie Backhus and Brian Linnane work to flip a 200-pound tire, while Field Office Chief Matt Roche (background) offers encouragement and Dan Finucane (right) keeps time.

LISTEN UP: Marine Staff Sgt. Thomas M. Lee, U.S. Marine Corps Martial Arts Center for Excellence instructor, provides a history and overview of the program to the Alexandria Field Office.

By Beth Alber
DSS Public Affairs Office

To get a better sense of how the DSS mission supports the warfighter, employees from Alexandria Field Office #1 travelled to Marine Corps Base Quantico for a day of briefings, exhibitions and a teambuilding event.

"I wanted the team to have a firm understanding of why it is so important to protect classified information and sensitive technologies being developed by our industrial base," said Matt Roche, Field Office Chief. "When they conduct their next assessment, I want them to be thinking about the Marines we met, and the military men and women who are end users of the technologies being produced."

The day started with a demonstration by members of the U.S. Marine Corps Martial Arts Center for Excellence (MACE). The goal of the MACE program is to "develop a professional Marine who is an arms-carrying-combatant who cannot only fight, but understands the moral dimensions of conflict, makes ethical decisions in any situation, and upholds the image and high moral fiber [of] the Corps."

While Marines demonstrated a variety of moves to disarm an enemy combatant, the Alexandria team was briefed on the history of the program, and the extensive and intensive training each MACE participant received.

"To get to that level, we are constantly training," said Marine Capt. Philip D. Palmer II, Operations Officer, MACE. "We have moved to high intensity, short duration workouts to simulate combat conditions."

After signing hold harmless agreements, the Alexandria team stepped out into the rain for the teambuilding exercise. As they broke into groups of four, Palmer explained the mission — work together to achieve success. The mission for each team was to either flip a 200-pound tire or drag a 250-pound chain for a distance of approximately 20 feet. Back and forth the teams went, taking breaks and switching places, as the rain turned the dirt into mud that made the going tougher as time wore on. A friendly competition broke out to see which team could flip the tire the most times during the time limit.

"I learned that success can't be achieved individually; in order to achieve any goal, you need the support of your

TAKEDOWN: Marine Staff Sgt. John D. Badon (left) and Marine Sgt. Daniel J. Leith, U.S. Marine Corps Martial Arts Center for Excellence instructors, demonstrate methods of disarming a combatant.

PUSH IT: Marine Capt. Philip D. Palmer II, Operations Officer, U.S. Marine Corps Martial Arts Center for Excellence, works with Sean Curran, Alexandria Field Office #1, to move the tire down the course.

WHAT A DRAG: William Ewald (left), of Alexandria Field Office #1, and Mike Farley, Capital Region Designated Approving Authority, drag a 250-pound chain as a part of a teambuilding exercise.

team members," said Annie Backhus, Industrial Security Specialist. "Our team was dedicated to completing the exercises, even with sheets of rain pouring down on us. We competed against each other, while still working together and having fun."

After successfully completing the event, the team settled into a conference room to discuss leadership. Palmer used personal experiences from his time in Iraq to discuss the aspects of leadership. In hindsight, he made his choices based on the information available even though it didn't always work out well. "As a leader, always be willing to give people a second chance," Palmer said. "Have people learn from their mistakes."

"The event enabled us to learn more about teambuilding," said Dan Finucane, Industrial Security Specialist. "Captain Palmer shared with us his views on how to properly lead a team, and the physical activity reinforced the necessity of working as a team by pitting us against challenges that required more than one person."

After the briefings, the Alexandria Field Office team toured the National Museum of the Marine Corps, which depicts the history of the Marine Corps and the battles fought through films, photographs, and graphically realistic displays.

"Today, we came away with a greater appreciation of the challenges Marines and our military face," said Roche. "We witnessed firsthand what strong teams can accomplish, and Captain Palmer demonstrated why it is so important that each individual on a team give 100 percent so that the man or woman on the left and right succeeds.

"Additionally, we realized that our ability to protect the information and technologies from a cyber-type event or unauthorized disclosure provides our military with an advantage," Roche continued, "and that strategic advantage means victory on the battlefield — which is what makes DSS so important."

Participating in the day's events from Alexandria Field Office #1 were Roche, Backhus, Finucane, Sean Curran, Lanie Peckar, Ryan Franklin, Brian Linnane, Emily Helstowski, William Ewald, and Stacey Williams. Also participating was Michael Farley, Capitol Region Designated Approving Authority. Alexandria Field Office members unable to attend were Linda Crossman, Ben Feldman, and Robin Nickel.

SAN ANTONIO FIELD OFFICE CHIEF RETIRES FROM MILITARY AFTER 28 YEARS OF SERVICE

Richard Hibbs, Field Office Chief for the San Antonio Field Office, retired from military service on June 1, 2012, after serving nearly 28 years in the United States Army (12 years) and U.S. Army Reserve (16 years).

Hibbs served primarily as a Military Intelligence Officer specializing in counterintelligence, strategic intelligence, and tactical intelligence collection. He was recalled to active duty in 2007 to 2008, serving with the 82nd Airborne Division and 101st Airmobile Division in Afghanistan as a part of Operation Enduring Freedom.

"I have worked for and with some amazing people in my 28 years; they epitomize the values you hold as a leader," he said. "They taught me to always surround yourself with people who are smarter than you and who are not afraid to make you think through the decision making process, and to always take care of your people."

His decorations include the Defense Meritorious Service Medal, Meritorious Service Medal with two oak leaf clusters, Army Commendation Medal with four oak leaf clusters, Army Achievement Medals with two oak leaf clusters, and numerous service and campaign decorations.

Hibbs began his DSS career in January 2001 in El Paso, Texas, as an Industrial Security Specialist, and he was promoted to Field Office Chief in October 2008. In that position, he supervises 10 personnel, whose industrial security duties cover Southern Texas (all areas East of El Paso; Waco and all areas south of Waco, and Southeast to the Gulf of Mexico and Louisiana border).

"I am humbled by the professionalism of the folks in the field office; they are a true inspiration to me," he said. "They have that 'can do attitude' and are willing to complete any task assigned to them."

He is a graduate of Indiana University, Bloomington, Indiana with a Bachelor of Science Degree in Public Administration with a concentration in Criminal Justice, and is a graduate of the U.S. Army Command and General Staff College.

"Serving your country has no greater calling whether in uniform or as a civilian." Hibbs said. "It was an honor for me to put on the uniform and to reflect on the people who paid the ultimate sacrifice for our country. My military time was an amazing ride and I would not trade one day of it."

PHOENIX FIELD OFFICE HOSTS DSS DIRECTOR

The Phoenix Field Office hosted Stan Sims, DSS Director, for a site visit in May 2012. Office personnel briefed Sims on the facilities within their areas of responsibility and shared their recent accomplishments.

Senior Industrial Security Representative Leslie Whitaker was named Industrial Security Field Operations Employee of the Quarter award and Sims recognized her accomplishment with a DSS Director's coin. Senior Industrial Security Representative Evelyn Romero was recognized by Western Region Director Karl Hellmann for successfully training three Industrial Security Representatives.

Industrial Security Representative Rob Glass, and Field Counterintelligence Specialists Jon Laahs and Nick Luce were recognized by Field Office Chief Jay Dixon for their partnership with cleared defense contractors in Southern Nevada. Together this trio identified the need for community relationship building, and initiated the formation of an NCMS chapter.

Previously, this area reported an average of four suspicious contact reports a year through 2010. Due to the efforts of these three individuals, contractors have reported more than 50 suspicious contract reports this past quarter, resulting in further actions by other government agencies.

VOLUNTEER EFFORT RECOGNIZED

Sara Ballard

Sara Ballard, Senior Industrial Security Specialist (ISS) in the Huntsville Field Office, was recently recognized for her volunteer efforts with the Red Stone Arsenal Army Community Service (ACS), for the seventh consecutive year.

Ballard first started volunteering in 1995, while at Fort Bragg, N.C., when she was asked to be a delegate for an Army Family Action Plan (AFAP) conference. It was there that she became aware of the Army Family Team Building (AFTB) program, which is a volunteer-led organization that provides training and knowledge to military spouses and family members.

The goal of AFTB is to improve personal and family preparedness, which enhances overall Army readiness and helps America's Army adapt to a changing world. When her husband transferred to Red Stone Arsenal in 2005 for a military assignment, Ballard renewed her volunteer efforts with ACS and the AFTB.

Although her husband has since retired from the military, Ballard continues to volunteer her time, and when possible, serves as a seasoned facilitator during the annual AFAP conference held every year.

"As a veteran, daughter of a veteran, mother of a veteran, sister of a veteran and a retired Army spouse, I have had numerous experiences over the years, in many parts of the world, and at times, I didn't know which way to go or who to speak with concerning matters of the military," Ballard said.

"Our country is enlisting families and because we are a Nation at war, those families need to be empowered and know what resources are available while their loved ones are deployed," she said. "While I may not have much to offer, I do have experiences I can share that will hopefully empower someone else."

Ballard began her career with DSS in September 2008, and in addition to serving as an ISS, she is certified to handle the Western Region Equal Employment Opportunity counselor duties. She was conferred the Security Professional Education Development, Security Fundamentals Professional Certification in February 2012.

Ballard has more than 34 years of combined military (six years active duty Army) and federal service, and has served in numerous locations overseas and stateside.

EMPLOYEES OBTAIN CERTIFICATIONS

Five DSS Information System Security Professionals (ISSPs) have completed requirements and obtained industry recognized certifications in cyber security and information assurance. These certifications formally document an individual ISSP's level of achievement and lend great credibility to the ISSP workforce in supporting the DSS mission.

Certified Information System Security Professional (CISSP) Certification

ISSPs John Fratturelli, Thomas LeBaron, and Jim Sexton recently completed a rigorous training and certification process to obtain Certified Information System Security Professional (CISSP) credentials. Candidates for CISSP complete a six-hour examination after meeting a number of pre-requisites including sponsorship into the program and a minimum number of years' experience in the information technology (IT) field.

A CISSP is an information assurance professional with the skills to define IT system architecture, management processes and procedures, and technical requirements to ensure security of information being processed on IT systems. The vast breadth of knowledge and the experience required to pass the CISSP exam is what sets it apart from other IT certifications.

The credential is a globally recognized standard representing competence in the areas of knowledge covered by the $(ISC)^{2®}$ Core Body of Knowledge (CBK). The CBK covers critical topics such as cloud computing, mobile security, application development security, and risk management. Achieving CISSP certification is an admirable accomplishment.

Obtaining and maintaining CISSP certification is a requirement to hold the position of DSS ISSP. The CISSP designation meets the requirement of DoD 8570.01-M, Information Assurance Workforce Improvement Program for Information Assurance Manager Level III.

"We have quite a few employees in the pipeline to obtain certification in the near future," said Randall Riley, Office of the Designated Approving Authority. "Well over half of the ISSP workforce already holds the CISSP credential. "Achieving certification as CISSP takes a lot of hard work, focus, and dedication," he continued. "It is an admirable accomplishment."

Certified Ethical Hacker (CEH) Certification

ISSPs Conrad Yanez and Max Shier recently completed the certification process to obtain the Certified Ethical Hacker (CEH) designation. CEH certification is a significant accomplishment beyond the CISSP and represents many hours of classroom and after-hours study to build upon an existing strong foundation of IT and networking knowledge.

The certification examination covers topics such as network perimeter defenses, network attacks, how intruders escalate privileges once inside the network, intrusion detection systems, security policy creation, social engineering, denial of service attacks, buffer overflows and malware creation.

The CEH designation meets the requirement of DoD 8570.01-M, Information Assurance Workforce Improvement Program, for Computer Network Defense Analysts and Incident Responders.

"This certification and the associated skill set directly support our mission and are quickly becoming more relevant given the new focus on Cyber Incident Response capabilities," said Riley. "The Certified Ethical Hacker designation is one of very few that documents an IT specialist is qualified to lead cyber incident response teams. While Conrad and Max are the first to achieve the certification, more ISSPs will pursue this certification in the future."

While ISSPs are focused on IT systems in industry, members of the staff the Office of the Chief Information Officer (OCIO) focus on the security of internal DSS networks and infrastructure.

The following OCIO employees, all members of the Information Assurance Division, also achieved CEH designation: Conrad Bovell, Chuck Robinson III, John Dangler, Chris Morton, Barbara Jackson, Ali Mohammed, Vinh Bui and Kim Moore.

SAN ANTONIO FIELD OFFICE
EMBRACES PARTNERSHIP WITH INDUSTRY

By Dawn Martin
Senior Industrial Security Specialist
San Antonio Field Office

The San Antonio Field Office has embraced the agency's philosophy of "Partnering with Industry." At every opportunity, our team goes the extra mile to ensure information and support flows to our industry partners, as well as to other government agencies. The following are examples of the recent events sponsored by the Field Office.

The Field Office recently hosted, "A Day with DSS" in Houston and Austin, Texas. At these two events, contractor and government personnel received, among other things, a DSS classified counterintelligence trends briefing; an advanced workshop on Chapter 8 of the National Industrial Security Program Operating Manual; training on safeguarding and closed area construction; clarification on how to complete the contracts list; an overview of security violations and reporting requirements; and a synopsis of "NISP [National Industrial Security Program] enhancements."

Working as a team, the Field Office created the briefings, and every member of the office participated, to include Richard Hibbs, Field Office Chief; Robert Ferrell, Information Systems Security Professional (ISSP); Peter Henning and Ron Wooten, Field Counterintelligence Specialists (FCIS); Betsy Bruinsma and Dawn Martin, Senior Industrial Security Specialists (SISS); and, Mery Neal, Rudy Sutton, Donna Heard and Jim Chituras, Industrial Security Specialists (ISS).

FCISs Henning and Wooten have provided numerous counterintelligence briefings to NCMS chapters, the FBI Infraguard program, the Office of Personnel Management, South Texas Counterintelligence Working Group, and the contractor communities in El Paso, Houston, San Antonio and Austin, Texas. Every briefing resulted in an increase in the reporting of suspicious incidents by those in attendance.

Field Office personnel consistently attend and participate in the local Texas NCMS chapter meetings and brown bag luncheons. Office personnel have taken these opportunities to advertise DSS initiatives, to include the new rating matrix system and NISP enhancements. In addition, office members have answered questions posed by industry and provided support as needed.

The Field Office volunteered to participate in the Partnership with Industry exchange program. A Raytheon Facility Security Officer spent a week in the office, learning about DSS through SISS Bruinsma and about the DSS counterintelligence program with FCIS Henning. In turn, ISS Heard traveled to Raytheon in Tucson, Ariz., to see the industry side of the industrial security business.

ISSP Ferrell provides information to the ISSM community on program changes and/or questions from industry. He encourages feedback and provides assistance in an effort to eliminate or reduce problems.

The San Antonio office also understands the importance of partnering with other government agencies. Office personnel, in conjunction with the Air Force Intelligence, Surveillance and Reconnaissance Agency Small Business Office, provide quarterly briefings to uncleared contractors who are interested in becoming part of the NISP. A step-by-step explanation on how to receive a facility clearance and what requirements exist after being cleared help attendees make a more informed decision on whether or not they want to bid on classified contracts.

SISS Martin provided a detailed presentation to the San Antonio Joint Base security office, consisting of government security specialists from three military installations. The presentation covered the NISP, facility clearances, the importance of submitting a comprehensive DD Form 254, computer systems, storage, security classification guidance, and the different requirements for contractors working on a military installation vice contractors working in their own facilities. The information enhanced the cooperative relationship between the government, DSS and cleared companies in the San Antonio community.

By using creative and innovative venues to tell the DSS story, the San Antonio Office continues to embrace "Partnership with Industry" by providing relevant information to contractors to ensure transparency and maintain open lines of communication.


DEFENSE SECURITY SERVICE