DSS ACCESS

VOLUME 2, ISSUE 4

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE

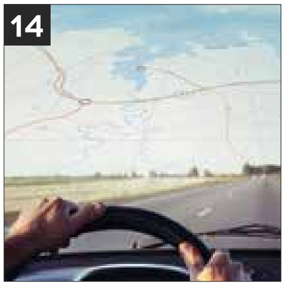
CDSE COURSES RECEIVE NEW ACCREDITATIONS EQUATING TO ADDED VALUE FOR STUDENTS

>> CONTENTS

WINTER 2013

VOLUME 2, ISSUE 4

14



31

33

SPOTLIGHT: CATCHING UP WITH CDSE

ASK THE LEADERSHIP

COMMUNICATION OF THE FUTURE

DSS CASE STUDY

INSIDE

DECIPHERING THE ACRONYMS

A HISTORICAL PERSPECTIVE

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.

The views expressed by the authors are not necessarily the official views of, or endorsed by, the U.S. Government, the DoD or the Defense Security Service.

All pictures are Department of Defense photos, unless otherwise identified.

FROM THE DIRECTOR

In this issue of ACCESS, we highlight the activities of the Center for Development of Security Excellence (CDSE). Our lead article notes their most recent achievement: Approval by the American National Standards Institute's (ANSI) — International Association for Continuing Education and Training (IACET) to award continuing education units (CEUs) for all courses in its program. This is a significant milestone for CDSE and DSS but more importantly an additional benefit for students of CDSE courses. Students benefit from CEUs as they provide a nationally established record of professional development and provide a method to document continuing education.

This new certification is just the latest example of how CDSE is looking forward and reevaluating its student population and how best to reach them with relevant training opportunities. For instance, we have an article that explores how technology is aiding the adult learner and delivering short, easily digestible training to busy professionals. We have another article that features the first students to complete CDSE's graduate level courses and how these security professionals intend to leverage their training to advance their careers.

We have an article looking at the recent top to bottom curriculum review CDSE undertook with subject matter experts from across the Department of Defense. This is a great example of soliciting and listening to our customers and stakeholders to deliver training that meets their needs. And finally, we highlight tools designed to help students prepare for the certification exams under the Security Professional Education Program.

CDSE may be leading the way with new thinking and methods, but the rest of DSS is not far behind as the articles on career mapping, the newest iteration of the security rating matrix, and the supervisor working group demonstrate. Working groups and internal initiatives such as these are great examples of how DSS can continue to deliver outstanding service in a fiscally constrained environment.

I continue to be impressed by the dedication and commitment of the men and women of DSS and the hard work evidenced on these pages. Thank you for all you do, and I look forward to an exciting 2014!

CDSE COURSES RECEIVE NEW ACCREDITATIONS EQUATING TO **ADDED VALUE FOR STUDENTS**

By Dr. Paul Krasley
Center for Development of Security Excellence

The Center for Development of Security Excellence (CDSE) has achieved another accreditation for its courses and programs. This further fulfills its role as the center of excellence for security education, training, and professionalization for the DoD and industry under the National Industrial Security Program (NISP). Students who complete certain courses through CDSE can reap three benefits beyond the lessons learned:

- Continuing Education Units (CEU) that can be applied toward maintaining a certification;
- Semester hours that can be used toward a college degree; and
- Professional Development Units (PDUs) that can be applied toward maintaining SPēD certifications.

International Association for Continuing Education and Training (IACET)

In July 2013, the CDSE received approval by the American National Standards Institute's (ANSI) International Association for Continuing Education and Training (IACET) to award continuing education units (CEUs) for all courses in its program.

CEUs provide a standard unit of measurement, quantify continuing education and training activities, and accommodate for the diversity of providers, activities, and purposes in adult education. Students benefit from the CEUs as they provide a nationally established record of professional development learning activity and provide a system to document continuing education experiences in meeting certification requirements.

The IACET accreditation came after an intensive, lengthy review process, for which CDSE provided over 350 pages of information on its programs. The programs were divided into 10 standard elements with details showing how CDSE met each element within the continuing education and training it provides.

CDSE was evaluated on its organization; responsibility/control/leadership; learning environment and support systems; event planning; learning outcomes; planning and instructional personnel; content and instructional methods, assessment of learning outcomes; how CDSE calculates and awards CEUs; learner records; and the overall program.

IACET's mission is to advance the global workforce by providing the standard framework for quality learning and development through accreditation. IACET helps government agencies develop a framework for continuous improvement and deliver a superior learning experience. IACET requires an annual review process, reaccreditation every five years, and for CDSE to maintain its level of excellence for each new course.

CDSE is already accredited by the Council on Occupational Education (COE). Both IACET and COE examine the entire CDSE organization including policies, processes, and procedures for consistency and excellence.

DoD policy requires that DoD civilian education and professional development activities meet the standards established by external accreditation and certification entities recognized by the U.S. Department of Education when applicable standards exist. COE accreditation is evidence that CDSE meets such standards. CDSE first won COE accreditation in 2002, reaffirmed accreditation in 2008 and will reaffirm accreditation once again in April 2014.

The American Council on Education (ACE)

In August 2013, five security training and five graduate-level courses offered by the CDSE were evaluated by the American Council on Education's (ACE) College Credit Recommendation Service (CREDIT) and were recommended for college credit. CDSE already had six training courses and seven graduate-level courses recommended for one to four semester hours of credit. CDSE will submit five more graduate-level courses and two more security-training courses during FY14.

National Commission for Certifying Agencies (NCCA)

CDSE received NCCA accreditation of its Security Fundamentals Professional Certification by demonstrating the program's compliance with the NCCA's Standards for the Accreditation of Certification Programs. NCCA is the accrediting body of the Institute for Credentialing Excellence (formerly the National Organization for Competency Assurance). Since 1977, the NCCA has been accrediting certification programs based on the highest quality standards in professional certification to ensure the programs adhere to modern standards of practice in the certification industry.

History

Accreditation emerged in the United States in the late 1800s as a voluntary peer review process initiated by educational institutions to assure quality. The goals of accreditation are to assure quality of the institution or program and to assist in the improvement of the institution or program. Accreditation within the United States is voluntary. The U.S. Department of Education provides oversight but "non-governmental" agencies like COE actually provide the accreditation.

Future

In the future, CDSE plans to explore the requirements necessary to grant degrees within the security discipline and therefore, join the ranks of other DoD institutions such as the service academies and other specialized DoD-related educational institutions.

AT RIGHT: Lower level means the first two years of a bachelor's degree program. Upper level means the second two years of a bachelor's degree program. Graduate level means a master's degree program.

Training		
Course Title	*Credit Hrs*	*Level*
DoD Personnel Security Adjudications	4	lower
Facility Security Officer Orientation for Non-Processing Facilities	2	lower
Facility Security Officer Program Management for Processing Facilities	2	lower
Introduction to Special Access Programs (SAP)	2	lower
Special Access Programs 2nd Tier Review	1	lower
SAP Mid-Level Security Management	3	lower
DoD Security Specialist Course Curriculum	3	lower
Applying Physical Security Concepts	3	lower
Information Security Management Curriculum	3	lower
Basic Industrial Security for Govt. Security Specialist eLearning	3	lower
Applying Physical Security Concepts eLearning Certificate	2	lower
Graduate		
Course Title	*Credit Hrs*	*Level*
Writing & Communications Skills for Security Professionals	3	grad
Security as an Integral Part of DoD Programs	3	grad
Organizational Consideration in Applying Security with the Federal & DoD Bureaucracy	3	grad
Constitutional Law and its Application to DoD Bureaucracy Security	3	grad
Understanding Adversaries and Threats to the United States and to the DoD	3	grad
Statutory, Legal, and Regulatory Basis of Defense Security Programs	3	grad
Challenges in Analyzing & Managing Risk	3	grad
Budgeting & Finance for Security Programs	3	grad
Human Resource Management for DoD Security	3	grad
Research Methods & Statistics to Support DoD Security Programs	3	grad
Assessment and Evaluation of a DoD Security Program	3	grad
Future of Security Systems & Information Assurance to Support DoD Security Programs	3	upper

CURRICULUM REVIEW SOLICITS FEEDBACK, GUIDES FUTURE CHANGE

The Center for Development of Security Excellence (CDSE) hosted its annual Curriculum Review meeting in September at the Pentagon Library and Conference Center. The event included participation from over 45 individuals from the Under Secretary of Defense for Intelligence (USD(I)), Joint Chiefs of Staff, military departments, combatant commands, Defense agencies, and activities. The purpose was to review curricula across functional areas as well as provide an opportunity for CDSE representatives to get firsthand feedback from community stakeholders.

To validate continued academic credibility, CDSE presented its recent accolades and awards. CDSE was the recipient of a Five-Star Award from the Federal Government Distance Learning Association, which recognized CDSE for "demonstrating excellence in providing enterprise-wide distance eLearning solutions."

In addition, CDSE courses were recognized with Omni and Horizon awards, for a total of 16 awards. CDSE continues its affiliation with the American Council of Education (ACE) and received additional ACE credit recommendations on three instructor-led courses and two eLearning curricula.

The meeting validated stakeholder support of webinars, eLearning courses, and security short format eLearning tools to better address immediate training needs. There was discussion on exploring alternative delivery methods to further meet the audience's time limitations. For example, attendees indicated that instructor-led courses may not, in some instances, be appropriate for their audience and suggested an eLearning course format be considered instead. CDSE agreed and discussed ongoing efforts to transition select instructor-led courses to a collaborative eLearning environment.

The meeting provided an excellent forum for discussion of future policy changes as well. Stakeholders mentioned various topical areas and policy changes that would ultimately require updated curriculum. Another topic of discussion was using webinars to immediately disseminate new policy to the community.

Stakeholders expressed satisfaction with CDSE's training courses and products and appreciated the opportunity to voice their questions and comments. Some involved with the Department of Defense Security Training Council commented they were pleased to see security standards identified in the Defense Security Skill Standards (DS3) aligned to CDSE courses. In a recent audit, CDSE courses were found to be in 96 percent alignment with the DS3.

According to Danny Jennings, the Physical Security and General Security curriculum manager, "Events such as the annual curriculum meeting aid CDSE in identifying potential training gaps and ensure they are responsive to community needs."

"EVENTS SUCH AS THE ANNUAL CURRICULUM MEETING AID CDSE IN IDENTIFYING POTENTIAL TRAINING GAPS"

DANNY JENNINGS

PHYSICAL SECURITY AND GENERAL SECURITY CURRICULUM MANAGER

SPēD certification exam? Need help? DSS developed tools to prepare

In July 2013, the Center for Development of Security Excellence (CDSE) launched Certification Preparatory Tools (CPTs) for the Security Fundamentals Professional Certification (SFPC) and Security Asset Protection Professional Certification (SAPPC) assessments.

The CPTs consist of three components. The first is a knowledge test. This tool presents a series of short-answer questions in each topic area covered on the SFPC and SAPPC assessments. Upon completion of the knowledge test, candidates are able to download a "review sheet" consisting of all the questions, master answers, and associated policies as well as resources available.

The second component is an experience checklist. Through a series of probing questions about experiences in each topic area, this tool assists candidates in evaluating their level of experience and determining their base of understanding in topic areas covered in the SFPC and SAPPC assessments.

Upon completion of the experience checklist, candidates are able to download a "learning resource guide," similar to the knowledge test, that identifies by topic area within each of the five security functional categories (general, industrial, information, personnel, and physical) the courses, information, and materials available to help increase proficiency. Finally, the CPTs also include a practice test that present examples of the type, difficulty, and format of the questions found on the SFPC and SAPPC assessments. In addition, it identifies the number of questions that will be tested in each topic area in the SFPC and SAPPC assessments.

"The CPTs promise to be a valuable resource in assisting security professionals prepare for SPēD Certification assessment," said Michael Scott, Professionalization Division chief, CDSE. "This online suite of tools will provide candidates with a means to better gauge their experience and evaluate their knowledge of the security competencies tested in the SFPC and SAPPC assessments."

The CPTs are available at: www.cdse.edu by selecting the link titled, "Prepare for SPēD Certification."

SPēD CERTIFICATION HITS NEW MILESTONES

SPēD Certification Program hits another milestone with **3,000** certifications conferred!

DSS has also successfully transitioned to using a commercial test vendor, with over **6,000** certification tests delivered.

With worldwide availability, the response from across DoD has been **outstanding**.

Today, the certification program has four certifications and one credential available:

- **Security Fundamentals Professional Certification;**
- **Security Asset Protection Professional Certification;**
- **Security Program Integration Professional Certification;**
- **Adjudicator Professional Certification**; and
- **Due Process Adjudicator Professional Credential**.

There are **four** more certifications in development and set for launch in FY14.

FIRST STUDENTS COMPLETE

Security professionals throughout the federal government and U.S. military services are taking advantage of the Center for Development of Security Excellence's (CDSE) curriculum of 17 semester-long graduate-level courses to prepare for leadership positions and responsibilities. The curriculum offers security professionals a unique opportunity to achieve academic and professional goals by attending courses delivered via an online collaborative learning environment. Students are able to experience the challenges, research, discussions, and critical thinking and analysis typical of university graduate-level courses.

The first course was offered in the summer of 2012 with 102 course completions since then. Seventy-nine students have completed at least one of these challenging courses and 15 students have completed at least two of them. CDSE has also packaged the courses into curricula that allow a student to earn a certificate by completing four courses.

Jeff Cooper, a program security manager with the U.S. Air Force is the first student to complete the requirements for one of the certificates, a certificate in risk management. Jeff advised, "Earning the certificate in risk management provided me the ability to execute cost benefit analysis to present vital information for leadership to make informed and effective decisions. This type of skill and knowledge can be applied across all of the security disciplines."

The courses allow students to work on real world issues and projects related to their mission. As an example, Jeff said, "I used the Challenges in Analyzing and Managing Risk course as my capstone project and conducted a risk management analysis on our base back gate to obtain funding for improvements to the base physical security measures."

Students took these courses for many different reasons including intellectual challenges, collaboration with security professionals throughout the federal government, and professional development to assist in career advancement. Kevin Cooper, a security specialist with the Department of the Navy completed two courses: Writing and Communication Skills for Security Professionals and, Security as an Integral Part of DoD Programs. He said, "The courses allowed me to gain more in-depth knowledge of security and allowed me to interact with other security professionals to discuss strategies." Kevin said he believes that security related graduate courses like this will benefit the careers of security professionals, adding, "Other security professionals would benefit by building on their skills to give them a step up the ladder to senior positions."

Dustin Frazier, a security specialist with the U.S. Army who completed multiple courses (Security as an Integral Part of DoD Programs, Organizational Considerations in Applying Security within the Federal and DoD Bureaucracy, and Understanding Adversaries and Threats to the United States) said, "In the course of completing three of these courses, I have analyzed the vast array of threats facing the DoD security community, learned effective methods to navigate the federal bureaucracy to achieve concise and effective security results, and gained a new appreciation of the emerging role of the multi-disciplinary security generalist as a career path. I look forward to broadening my knowledge base as I continue to progress through this program."

The courses are offered to U. S. military members and Federal government employees without charging any tuition or fees. Frazier said he "would highly encourage security professionals to take advantage of these training opportunities. Given the budgetary constraints facing the government today, this program represents a unique opportunity for security professionals to earn graduate-level certificates in a variety of security-related fields, acquire Professional Development Units to maintain SPēD certifications, facilitate the exchange of new ideas and best practices to counter complex security challenges, and acquire the skill-sets necessary to become effective practitioners of security. All of these benefits are available to applicants at little or no cost to their respective organizations. As I said, I have not found a more beneficial training program for security professionals than what is offered through these courses."

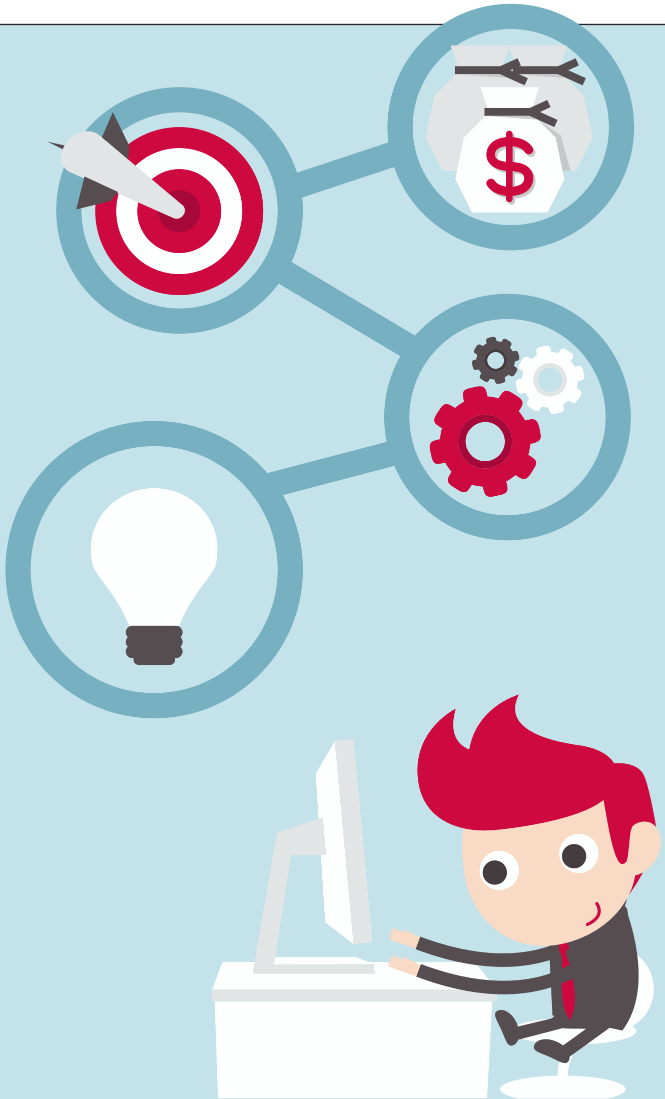
Eleven of the CDSE Education Division graduate-level courses have received American Council on Education (ACE) Credit Recommendations in the graduate degree category for three semester hours. The remaining courses will be reviewed by ACE in the coming months. Information about the ACE College Credit Recommendation Service can be found at the ACE web site: www.acenet.edu. CDSE courses that have been

GRADUATE-LEVEL COURSES

reviewed by and have received recommendations from ACE are listed at: www2.acenet.edu/credit/?fuseaction=browse.getOrganizationDetail&FICE=1007408.

Approximately 80 students are participating in the fall semester of classes, and the Winter 2014 semester begins Jan. 6, 2014. The DSS website offers more details about the CDSE Security Professional Education program, including course descriptions, dates, prerequisites, and enrollment information at www.dss.mil/education/index.html.

- **Writing and Communication Skills for Security Professionals** where students explore the skills and behaviors that DoD Security Professionals need to succeed using oral and written communications.
- **Security as an Integral Part of DoD Programs** where students explore the cross-disciplinary functions that support the missions of DoD commands and agencies.
- **Organizational Considerations in Applying Security within the Federal and DoD Bureaucracy** where students take an in-depth look at how to work within the Federal and DoD bureaucracy to accomplish security missions.
- **Constitutional Law and its Application to DoD Security** where students study cases and examine governmental authority.
- **Understanding Adversaries and Threats to the United States and to DoD** where students examine the multifaceted concept of threat and explore the intentions and capabilities of adversaries to the United States and to DoD.
- **Budgeting and Financial Management for Security Programs** where students study financial management through applied security problems and case studies.
- **Human Resource Management for DoD Security** where students gain in-depth knowledge and understanding of Human Resource Management and the skills and tools needed to make effective decisions.
- **Security in the DoD Acquisition Process** where students examine the basics of the acquisition process and the various security roles and responsibilities within the acquisition process.
- **Research Methods, Data Analysis, and Reporting to Support DoD Security Programs** where students examine research strategies, designs, data collection, and reporting techniques used to justify resources and evaluate research proposals.
- **Assessment and Evaluation of DoD Security Programs** where students establish and share concrete achievements and measurements that effectively demonstrate the impact of security programs and activities.
- **The Future of Security Systems and Information Assurance** where students who work in the security field examine leading-edge technologies and their implications for the field of security within DoD.
- **Leadership in DoD Security** where students gain in-depth knowledge, skills and understanding of leadership principles and skills needed to support DoD security programs.
- **Effective Communication in DoD Security** where students explore effective techniques for communicating ideas, concepts, and policies in defense security.
- **Managing a DoD Installation Security Program** where students examine how the use of risk-management techniques and DoD security requirements lead to the development of a comprehensive, capabilities-based installation security plan.
- **Cybersecurity and Oversight of Information System Security** where students explore how the role of the non-technical DoD security specialist relates to information systems security, information assurance and cybersecurity.
- **Statutory, Legal, and Regulatory Basis of DoD Security Programs** where students explore the specific statutes, regulations, and Executive Orders driving the establishment and implementation of DoD and Federal security programs.
- **Challenges in Analyzing and Managing Risk** where students examine risk management theory, DoD risk management practice and risk management decision-making methodology in dealing with imminent security threats.



ADULT LEARNERS

In 2000, training at the Defense Security Service (DSS) consisted of an instructor standing in front of a group of people and a few mailed CD's with PDF versions of correspondence courses.

Now, the Center for Development of Security Excellence (CDSE) has over 94 electronic learning courses listed online, over 26 security "shorts" deployed, more than 38 archived webinars, and 17 education online courses. These are in addition to 14 instructor-led courses.

How is CDSE able to leverage technology to aid the training and instruction to students? Here are some examples of how CDSE came together, as a team, to tackle issues working with adult learners in 2013.

DSS is partnering with the Defense Information Systems Agency (DISA) to leverage the Defense Connect Online (DCO) to provide live presentations through webinars. The webinars are focused on specific topics and issues of interest to the security community and often reach up to 1,000 listeners per session. They are scheduled to be about half an hour in length with two sessions to allow participation during lunch breaks on both the east and west coasts. Webinars are also archived for those who may have missed the live event.

Current CDSE students and stakeholders requested separate training/awareness packages which were short in duration and

EDUCATIONAL TECHNOLOGY BRANCH:

MEET THE PEOPLE BEHIND THE COMPUTERS

By embracing technology, DSS and the Center for Development of Security Excellence (CDSE) have successfully moved from a classroom based instructional model to an on demand delivery method. Even with the best technology, this transition would not be possible without a staff of designers, developers, and programmers.

Johnson

The Educational Technology branch (Ed Tech) is part of the Multimedia Productions division at CDSE. The EdTech branch is focused on building and maintaining the interactive, web-based systems that aid in the learning process.

The branch supports the development of short-format learning development modules and provides a technical support arm for the Security Professional Education Development (SPēD) certification process. Ed Tech also maintains the CDSE external website.

Branch personnel work closely with the other divisions in CDSE, within DSS, and outside agencies to develop training and awareness products. One tool Ed Tech created included a virtual environment that

BENEFIT FROM NEW TECHNOLOGIES

focused on a small topic area. To meet this need, CDSE produces 'Security Shorts'. These 'shorts' are usually ten minutes in length or less and are posted to the CDSE web site for anyone to access. Topics covered in the shorts include key bits of information on counterintelligence, industrial security, information security, personnel security, physical security, special access programs, and general security topics.

Stakeholders are free to integrate these shorts into their internal security awareness programs. For example, one security officer has directed employees with security clearances in his area to review 'The 13 Adjudicative Guidelines' short as a reminder of areas they should be aware of to maintain their security clearance access.

By leveraging technologies and advancements made by the gaming industry and virtual simulation companies, CDSE is able to provide students with access to systems and components regardless of their physical location. CDSE is able to create learning environments which simulate real-world conditions while at the same time providing feedback to the student.

For example, a security officer in a virtual training tool could find themselves in the hallway of a typical office space. They would be able to navigate the virtual building looking for security deficiencies, but just as in the real world, the student wouldn't see an arrow or glow around an unsecured safe left unattended. They could make notations on any security deficiencies they identified and receive feedback on the items they got correct as well as any they might have missed.

CDSE is also moving instructor-led courses to an online, collaborative learning environment. This will allow students to gain the required level of interaction with the instructor, but through a virtual classroom learning system.

Using this environment, the instructor will provide weekly audio/video instruction segments and assign work and exercises to the students. The system will also allow the students to collaborate and work together on team projects. The virtual collaboration system will provide the students access to the system at times during each school week depending on their schedule.

As the use of technology continues to change, CDSE has a plan to continue moving forward in embracing and adapting that technology to fits the needs of its students. CDSE will also continue to look for ways to provide a worldwide base of students and visitors access to the training and education materials they need, when they need it, in a format that meets their needs.

Lord

Lynn

Weisz

Vice

Zambrowicz

allowed students to interactively inspect rooms and buildings. The immersive 3D environment even allowed students to climb a ladder to inspect the ceiling of a room. Ed Tech also worked with the Army to develop training used DoD-wide.

The branch consists of a team of very talented individuals who bring years of experience and diverse backgrounds: **Lori Johnson** has developed numerous courses and advocates use of new technology to speed course development and improve learner experience. **Susan Lord** uses her strong instructional system design background to create numerous interactive learning environments for CDSE students. **Stephen Lynn**, **Rene Weisz** and **Melissa Vice** are programmers and designers who have developed the 3D learning environments. **Caroline Zambrowicz** is a web programmer and was the lead developer in the redesign of the DSS.Mil website.

A Q&A WITH **DREW WINNEBERGER**,

Drew Winneberger is currently the director of Industrial Policy and Programs. He joined the Defense Security Service in March 2008, serving as a senior advisor on a range of counterintelligence and security matters.

Before joining DSS, Winneberger was the Director of Counterintelligence and Security for the Defense Intelligence Agency (DIA). His professional experience includes personnel security, physical and technical security, information security, and counterintelligence support. Prior to his career at the DIA, he served as a counterintelligence agent with the U.S. Army.

Industrial Policy and Programs (IP) includes functions such as Policy, International, Special Access Programs, Assessment and Evaluations and Foreign Ownership Control and Influence (FOCI). Some of these functional areas may not be well understood. Can you briefly describe each one and their role?

The Policy office is responsible for interpreting policy for the field and industry. This is accomplished through the issuance of Industrial Security Letters (ISLs). These ISLs are often the basis for subsequent revisions to the National Industrial Security Program Operating Manual (NISPOM). One of the most important responsibilities of this shop is to respond to questions from the field on the correct interpretation of specific provisions of the NISPOM. Since policy, no matter how well written, can't possibly anticipate all scenarios.

The Special Access Programs (SAP) office is responsible for coordinating all aspects of DSS support to very sensitive SAPs. This is a very important, sensitive mission area that operates strictly on a need-to-know basis and by necessity, must maintain a low profile.

The International division oversees and administers guidelines regarding cleared U.S. contractor involvement with foreign governments, foreign contractors and NATO. This is a very busy, but little understood activity. Anytime a cleared company desires to transfer classified material to a foreign country in support of an authorized exchange, the International division must approve the transportation plan for the material and seek approval from the foreign government receiving the material. For some of our largest contractors, it can be a high volume activity. In addition, the division passes and receives clearances associated with authorized foreign visits to U.S. contractors and U.S. contractors visiting a foreign facility. Finally, the International division ensures that foreign classified information, in the possession of cleared U.S. contractors, is protected in accordance with the foreign government's requirements.

The Assessments and Evaluations division (A&E) is our financial analysis and oversight office. Many people don't realize the government, through DSS, pays for the personnel security clearances for industry personnel cleared under the National Industrial Security Program (NISP). The A&E division is charged with overseeing the execution of this approximately $240 million annual program. They monitor on a weekly basis the execution of these funds to ensure DSS does not run out of money for this critical program. To support budget development, A&E conducts an annual survey of the approximately 13,000 facilities in the NISP to determine budget requirements for the following year. Historically, this survey has been accurate within five percent. A&E also participates in the continued monitoring of companies entering the NISP.

The FOCI Operations division (FOD) and FOCI Analytical division (FAD) are probably the most high-profile offices in IP. With the increasing globalization of the U.S. industry, more and more foreign investment is attracted to the U.S. defense market. The FAD, in addition to analyzing FOCI cases, reviews every company entering the NISP. Once in the NISP, the FAD, in coordination with A&E, performs continuous monitoring of the companies to detect any information that may impact the continued clearance of facility. The FAD FOCI analysis is vital to the overall decision process that the FOD uses when addressing FOCI mitigation. The FOD staff works closely with DSS field personnel and company officials in negotiating the mitigation plan. These are often very complex negotiations that involve an in-depth understanding of corporate structures and governance. Once the plan is in place, FOD personnel often participate with field personnel in the subsequent security vulnerability assessments and annual board meetings.

How do these disparate functions work together to advance the industrial security mission and support Field Operations?

Virtually everything that IP does is in direct support of Field Operations. With the workload in the field, where the ratio of facilities to the representatives is approximately 75 to 1, it is important that we provide timely, accurate support. We have to be a force multiplier for the field so they can maximize their assessment time at facilities. Nearly every division has a requirement to visit field offices and participate in assessments which gives IP personnel a better appreciation of the day-to-day challenges faced in the field.

Can you describe some of the changes IP has made in the FOCI mitigation process? How have these changes improved the process?

Early in Mr. Sims' tenure as Director, he charged the mission activities, such as IP, to improve the consistency of the DSS processes across the regions. To address these concerns, IP moved toward a model of centralized management with decentralized execution. By changing the way various processes are managed, we help ensure consistency in the FOCI process.

For example, questions of colocation of cleared entities with foreign affiliates and possible shared services are adjudicated by the FOD with input from Field Operations. Once these issues are adjudicated, Field Operations assumes responsibility for the oversight. The centralized adjudication of these issues contributes to a more uniform application of processes. We are currently reviewing other processes which lend themselves to this model.

How has the role of foreign investment in the defense industrial base changed and what steps do you take to determine whether foreign investment poses a national security threat?

With the global downturn in the world economy, the U.S. defense market remains one of the most lucrative in the world. For this reason, foreign investors will continue to pursue opportunities to invest in this market. At the same time, the contraction of defense spending is forcing many U.S. contractors to seek an infusion of capital to offset this market decline and to provide them with more opportunities for involvement in global markets. One of the functions of the FAD and A&E is to analyze who the players are involved in the foreign investment in cleared industry and determine the threat posed. All of these factors are evaluated on a case-by-case basis. However, sometimes it is difficult to precisely determine the origin of the foreign investment when private equity firms or sovereign wealth funds are involved.

How is the analysis IP is doing — whether in FOCI or Assessments and Evaluations — helping identify vulnerabilities in the defense industrial base and recommending strategies to mitigate the risks?

Until recently, companies entering the NISP were subject to very little scrutiny other than some basic determinations regarding being legal entity in the U.S. and sponsored by a government contracting activity. As the analytical capability of IP has grown, we have been able to introduce a more rigorous process. Between the FOCI Analytical division and the Assessment and Evaluations division, a myriad of databases, both classified and unclassified, are routinely checked before a company can be granted a Facility Clearance (FCL). Examples of the issues IP discovered include:

- The company is no longer authorized to operate in the state due to State tax problems
- Unreported issues of Foreign Ownership, Control, or Influence
- The company has been debarred from doing business with the DoD as the result of fraud or other criminal activity
- Unreported changes in Key Management Personnel

Once the company is in the NISP, they are subject to continuous monitoring to detect any problems that may occur. We no longer depend solely on the company to report issues. We are more proactive than reactive. For instance, our weekly publication, "NISP Facility Oversight" is designed to alert DSS field personnel to potential problems with facilities under their responsibility.

All of this analysis provides the primary benefit of allowing IP to tailor risk mitigation plans to the specific threats associated with a particular contractor.

What is the biggest challenge for IP?

Like many areas in DSS, we are challenged by an increasing workload with static resources. I try to encourage creative thinking and problem solving that forces us to look for innovative ways to improve our processes. We are constantly looking for data sources that will allow us to make the most informed recommendations for risk mitigation. The IP team aggressively pursues a wealth of mostly open-source information as well as other tools that allows us to effectively aggregate information in our analysis.

In the area of FOCI, we are virtually the only DoD component doing this type of work. In many regards, we are blazing new trails in the work we do. This allows us to develop our own processes and problem solving routine. As a result of this work, DSS is quickly establishing a reputation as a center of excellence for all matters related to FOCI and financial analysis.

CAREER MAPPING ENSURES PEOPLE ARE PRIORITY

When Theodore Banks joined the Industrial Policy and Programs (IP) directorate, it was his hope that he was not just starting a new job but embarking on a career. Banks found though that there was no clear cut path or guide to help him navigate his career. With time and considerable effort, he figured it out on his own. He hoped for a more transparent process for his colleagues and those who came after him.

DSS recognizes the critical role of people-power in the modern national security environment. This is why DSS undertook the Career Mapping Initiative (CMI), which is focused on the professional development of its most valuable asset: people. The purpose of the CMI was to create a framework to help employees develop the knowledge, skills, and abilities to progress, and empower them to develop their own careers and better deliver on the national security mission.

“No one really knows exactly where they’ll end up in their careers, but having a tool to guide some of the natural career ambiguity will help employees,” said Banks.

Taking Action

Banks’ story is not unique to DSS. His is a challenge many employees within the defense intelligence industry face: how to navigate a career while also serving the mission and the public?

“We realized year after year we were losing great talent to other organizations. It is important for any business or government agency to be able to retain their top talent, and we were not doing that effectively. Moreover, we had data to suggest that employees were disengaged and perhaps leaving DSS for that very reason. Once you can identify a problem it makes it much easier to solve,” said La Shawn Kelley, Chief of the Human Capital Management Office (HCMO).

DSS went straight to the source and asked the employees what they wanted and needed to make their careers at DSS successful. Employees responded by telling leadership they were hungry for career development, to grow their individual and collective potential in line with the future vision of the agency. DSS listened and kicked off the CMI.

DSS HCMO led the effort — with the participation of over 150 employees — to develop career maps for 11 mission critical occupations which accounts for approximately two-thirds of the DSS workforce. The occupations are: Curriculum Manager; Cyber Counterintelligence Analyst; Cyber Counterintelligence Liaison Officer; Field Counterintelligence Specialist (FCIS); Field Office Chief; Foreign Ownership, Control or Influence (FOCI) Analyst; FOCI Operations; Industrial Security Representative; Information System Security Professional; Instructor; and Intelligence Analyst.

“I was eager to participate in this initiative,” said Dana Richard of the Counterintelligence directorate. “We wanted to create our own Counterintelligence career framework for a while and even started drafting it! To have a coordinated effort to do it not only for us, but for the other directorates across the agency is a welcomed outcome.”

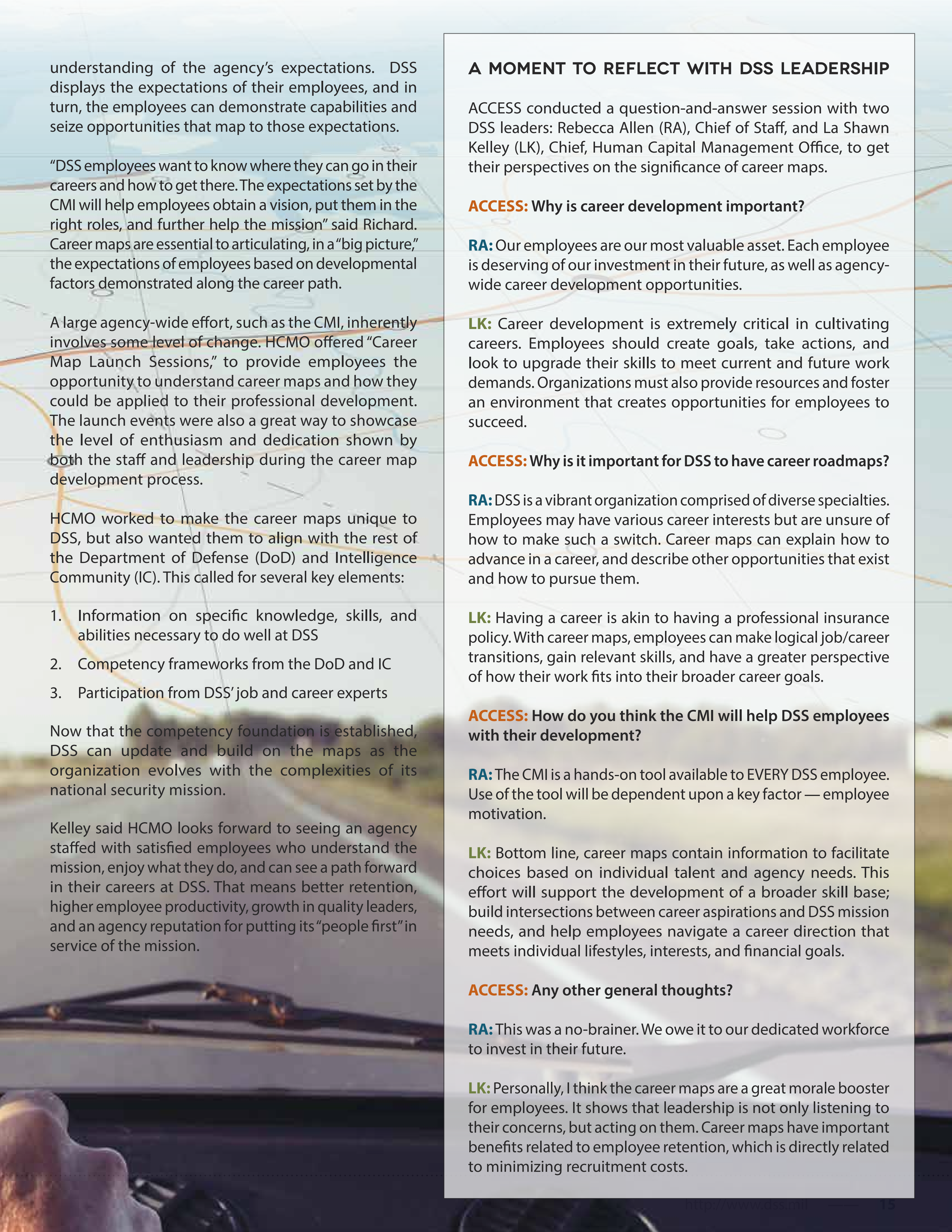
The Career Mapping Initiative

The CMI applied a rigorous, data-driven process to create the career maps. The goals of the CMI were simple.

1. Guide employees to achieve their professional goals and help provide an effective starting point for collaborative career planning
2. Equip DSS with a competency foundation to build an agile workforce
3. Help DSS employees recognize skill sets to strengthen individual and agency-wide capabilities

How It Works

When employees use the career maps, they gain a better



understanding of the agency's expectations. DSS displays the expectations of their employees, and in turn, the employees can demonstrate capabilities and seize opportunities that map to those expectations.

"DSS employees want to know where they can go in their careers and how to get there. The expectations set by the CMI will help employees obtain a vision, put them in the right roles, and further help the mission" said Richard. Career maps are essential to articulating, in a "big picture," the expectations of employees based on developmental factors demonstrated along the career path.

A large agency-wide effort, such as the CMI, inherently involves some level of change. HCMO offered "Career Map Launch Sessions," to provide employees the opportunity to understand career maps and how they could be applied to their professional development. The launch events were also a great way to showcase the level of enthusiasm and dedication shown by both the staff and leadership during the career map development process.

HCMO worked to make the career maps unique to DSS, but also wanted them to align with the rest of the Department of Defense (DoD) and Intelligence Community (IC). This called for several key elements:

1. Information on specific knowledge, skills, and abilities necessary to do well at DSS
2. Competency frameworks from the DoD and IC
3. Participation from DSS' job and career experts

Now that the competency foundation is established, DSS can update and build on the maps as the organization evolves with the complexities of its national security mission.

Kelley said HCMO looks forward to seeing an agency staffed with satisfied employees who understand the mission, enjoy what they do, and can see a path forward in their careers at DSS. That means better retention, higher employee productivity, growth in quality leaders, and an agency reputation for putting its "people first" in service of the mission.

A MOMENT TO REFLECT WITH DSS LEADERSHIP

ACCESS conducted a question-and-answer session with two DSS leaders: Rebecca Allen (RA), Chief of Staff, and La Shawn Kelley (LK), Chief, Human Capital Management Office, to get their perspectives on the significance of career maps.

ACCESS: Why is career development important?

RA: Our employees are our most valuable asset. Each employee is deserving of our investment in their future, as well as agency-wide career development opportunities.

LK: Career development is extremely critical in cultivating careers. Employees should create goals, take actions, and look to upgrade their skills to meet current and future work demands. Organizations must also provide resources and foster an environment that creates opportunities for employees to succeed.

ACCESS: Why is it important for DSS to have career roadmaps?

RA: DSS is a vibrant organization comprised of diverse specialties. Employees may have various career interests but are unsure of how to make such a switch. Career maps can explain how to advance in a career, and describe other opportunities that exist and how to pursue them.

LK: Having a career is akin to having a professional insurance policy. With career maps, employees can make logical job/career transitions, gain relevant skills, and have a greater perspective of how their work fits into their broader career goals.

ACCESS: How do you think the CMI will help DSS employees with their development?

RA: The CMI is a hands-on tool available to EVERY DSS employee. Use of the tool will be dependent upon a key factor — employee motivation.

LK: Bottom line, career maps contain information to facilitate choices based on individual talent and agency needs. This effort will support the development of a broader skill base; build intersections between career aspirations and DSS mission needs, and help employees navigate a career direction that meets individual lifestyles, interests, and financial goals.

ACCESS: Any other general thoughts?

RA: This was a no-brainer. We owe it to our dedicated workforce to invest in their future.

LK: Personally, I think the career maps are a great morale booster for employees. It shows that leadership is not only listening to their concerns, but acting on them. Career maps have important benefits related to employee retention, which is directly related to minimizing recruitment costs.

NEW CERTIFICATION DEVELOPED FOR INDUSTRIAL SECURITY OVERSIGHT PRACTITIONERS

The Industrial Security Professional Oversight Certification (ISOC) is a new specialty certification under the auspices of the Security Professional Education Development (SPēD) program. The ISOC was developed specifically for individuals with DoD industrial security oversight duties and responsibilities to understand and apply associated concepts, principles, and practices. The primary audiences for this certification are employees of the Defense Security Service and the DoD components.

The certification assessment focuses on select skill standards and competencies linked to foundational concepts specific to industrial security oversight. These include, but are not limited to:

- General Security
- Incident Response
- Industrial Security
- Information Assurance/Cyber Security
- Information Security
- National Industrial Security Program
- Personnel Security
- Physical Security

For the DSS population, the ISOC addresses foundational concepts in the facility security and clearance arena, and includes skill standards and competencies linked to:

- General safeguarding requirements
- Facility surveys
- Security inspections

The ISOC beta test launched on July 8, 2013, and concluded on Aug. 30, 2013. The initial test consisted of 238 questions within a two-hour time limit and was offered through Pearson VUE commercial testing sites worldwide. DSS Industrial Security representatives participated in development of the beta test questions.

A total of 313 candidates registered for the beta test, and 97 DSS employees, representing multiple directorates, registered for the assessment; fully one-third of the total population.

The ISOC is expected to be in full-production sometime in December 2013, after the Beta data is analyzed and a final vote is made by the DoD Security Training Council.

REVISED SECURITY RATING MATRIX TOOL IMPROVES CONSISTENCY, FURTHER DEFINES ENHANCEMENTS

The changes to the matrix included:

Updated definitions for each enhancement to include explicitly outlining the intent, allowing DSS and industry to focus on the purpose behind the category and more easily identify examples.

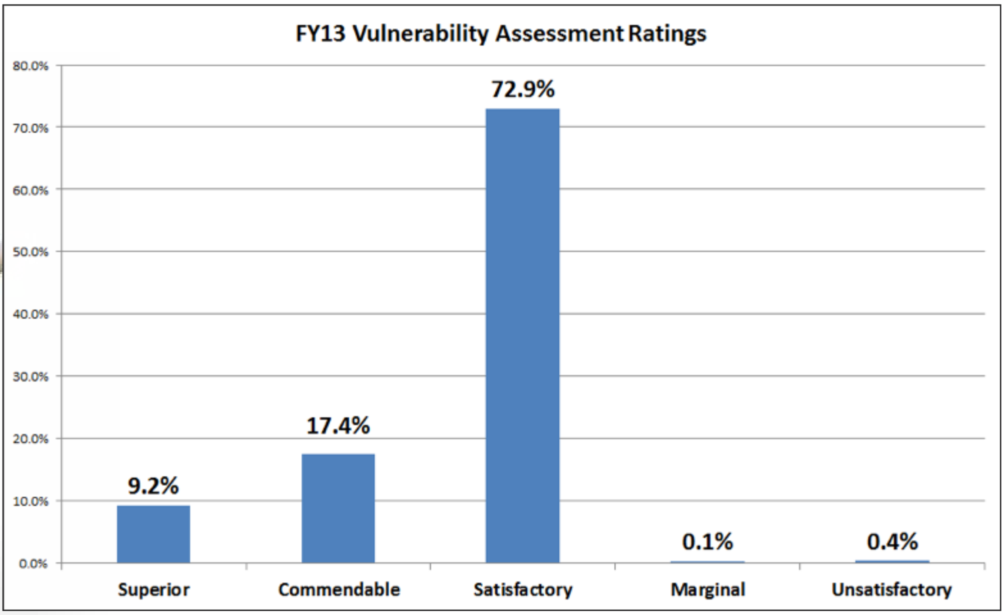
Additional examples of activities that would fall under enhancement categories.

A reduced amount of categories (10 vs. 13) enables more consistent and equitable ratings across all types of facilities in the NISP.

- To reduce overlap in enhancement activities, the combined categories include "International" and "FOCI" (now "FOCI/International") and "Membership/Attendance in Security Community" with "Active Participation in Security Community" (now "Active Membership in Security Community")
- To focus on NISP-enhancing security benefits and achievability, removed "Personnel Security"

A revised scoring process that more equitably rates facilities by large possessor, small possessor, non-possessor, and takes into consideration the reduction in enhancement categories.

Below is a summary of the assessments performed and ratings granted in FY 13:



DSS and industry had long recognized the need for a standardized, less subjective rating process. And in November 2011, the security rating matrix calculation tool was introduced to standardize and improve rating consistency.

It is numerically based, quantifiable, and accounts for all aspects of a facility's involvement in the National Industrial Security Program (NISP). It provides full transparency on how DSS arrives at ratings, assessing impact of a security program's vulnerabilities (non-compliance with National Industrial Security Program Operating Manual [NISPOM] standards) and enhancements.

The initial introduction of the rating matrix was a well-received success, but DSS remained committed to further enhancing the matrix and incorporating lessons learned.

A critical component of the matrix is the concept of a NISP enhancement. An enhancement directly relates to and enhances the protection of classified information beyond baseline NISPOM standards. NISP enhancements are validated during assessments as having an effective impact on the overall security program and are normally accomplished through employee interviews and review of process/procedures.

NISP enhancements are broken out in categories based on practical areas to provide clear definitions to industry partners and ensure field oversight consistency with the goal of encouraging facilities to implement well-rounded security programs. The aim is to give credit to the true impact of the security enhancements, rather than to attempt to consistently break-down each isolated event. Examples of categories include security staff professionalization, counterintelligence integration, and classified material controls.

DSS considers some items, if identified during the assessment, as a "red flag area," and the rating matrix score may no longer be applicable. For instance, vulnerabilities of unmitigated Foreign Ownership, Control or Influence (FOCI) or uncleared key management personnel may affect the overall facility security clearance status. If these items are identified, the field representative will not assign the security rating at the conclusion of the assessment, and DSS internal coordination will take place.

Since early 2013, DSS has worked between field personnel and industry partners to update the rating matrix, incorporating best practices and feedback to achieve an even more transparent, consistent and objective process. In January 2013, four field offices (one per region) participated in a pilot of the updated rating process. During the pilot, industrial security representatives and information system security professionals supplemented the current rating process with the revised tools on their scheduled assessments. Overall, the new process led to further improvements in consistency and additional clarity in enhancements and vulnerabilities. The revised matrix was launched in September.

To help industry understand the new system, DSS created a document covering the entire rating matrix. It outlines the assessment process, vulnerability definitions, and enhancement categories. Find the document at: www.dss.mil/documents/facility-clearances/Vuln_Assm_Rating_Matrix_2013_Update.pdf.

ACCESS
GRANTED

DEADLINE LOOMS FOR TRANSITION TO ELECTRONIC FINGERPRINT CAPTURE & SUBMISSION

By Zaakia Bailey
Personnel Security Management Office for Industry

In a memorandum dated July 29, 2010, the Under Secretary of Defense for Intelligence issued a requirement that Department of Defense (DoD) components transition to electronic capture and submission of fingerprint images in support of all background investigations by December 31, 2013. As of August 2013, cleared companies submitted 54,727 fingerprints by hard copy and 18,077 fingerprints electronically to the Office of Personnel Management (OPM).

In an effort to comply with this mandate, DSS outlined options for industry to submit fingerprints electronically to initiate background investigations. Industry may implement one or more options based on funding, mission needs and geographic locations.

Option 1: Company Purchases Equipment

Companies purchase electronic fingerprint capture/hardcopy scanners in order to submit fingerprints electronically to Secure Web Fingerprint Transfer (SWFT).

Option 2: Company Shares Resources

Multiple companies share the cost of purchasing electronic fingerprint capture/hardcopy scan devices.

Option 3: Company Offers Service

Cleared companies support other companies by submitting electronic fingerprints to SWFT. Companies providing the service of uploading fingerprints to SWFT may submit all fingerprint files under their CAGE Code.

Option 4: Third Party Vendor Provides EFT File

Companies receive the electronic fingerprint (EFT) file from a third party vendor that is an FBI-approved channeler. The third party vendor collects the fingerprints and saves the file in the required format to meet SWFT, OPM and FBI standards.

Option 5: Other Government Entities

Industry can partner with the military services and other government agencies participating in the National Industrial Security Program for electronic fingerprint submissions. Military services and government agencies may leverage their electronic processes to submit the fingerprints directly to OPM.

Next Steps

As the deadline nears, Department of Defense collaboration with and continued support of industry security professionals will be critical to the successful transition to an electronic fingerprint process.

DSS posted an updated Electronic Fingerprint Capture Options for Industry guide, which outlines all the options available, as well as frequently asked questions on its website at www.dss.mil/psmo-i/index.html

In an effort to further assist companies, the DSS Personnel Security Management Office for Industry (PSMO-I) has been hosting webinars outlining e-Fingerprint options for industry.

Facility Security Officers should visit www.dss.mil/psmo-i/indus_psmo-i_webinars.html or email AskPSMO-I@dss.mil for more information regarding upcoming webinars. The Defense Manpower Data Center posted SWFT approved vendors to the SWFT homepage. This information is of specific benefit to companies opting for Options 3 and 4. The PSMO-I staff will continue to answer questions related to e-Fingerprint and SWFT requirements, as well as educating industry when they request hardcopy fingerprint cards.

INTERNATIONAL DIVISION

NEW MISSION RESPONSIBILITIES

International Outgoing Visit Requests

Classified visit requests to foreign military, government and industrial sites in approximately 69 countries

NATO visit requests to over 50 locations in the U.S. and overseas

Facility Requests/Verifications

Foreign Facility Security Clearance (FSC) requests

Issuance of NATO Facility Security Clearance Certificates (NFSCC) to NATO agencies

Personnel Security Assurances/Clearances

NATO Security Clearance Certificates for U.S. Citizens hired by NATO agencies

Personnel Security Clearance Verifications for U.S. citizens within and outside NISP

Limited Access Authorizations (LAA) Secret requests for foreign nationals

Requests for NATO Security Clearances for foreign nationals

Foreign security assurances for foreign nationals who have lived or resided in the U.S.

On April 1, 2013, the International Division of Industrial Policy and Programs went live with the new assurance mission that was stood up as a result of the DoD Central Adjudicative Facility (CAF) consolidation.

The CAF consolidation, directed by the Deputy Secretary of Defense in May 2012, brought together the functions, resources, and assets of the Army Central Clearance Facility, Department of the Navy CAF, Air Force CAF, Joint Staff CAF, Washington Headquarters (WHS) CAF, Defense Industrial Security Clearance Office (DISCO), and the Defense Office of Hearings and Appeals (DOHA) into a single organization under the authority, direction and control of the Director of Administration and Management.

However certain non-adjudicative responsibilities, such as Security Assurances, were retained by DSS and transitioned from DISCO to the International Division.

Preparation for this transition required extensive planning and coordination with the CAF, as well as recruitment of a new staff and training within a compressed timeframe to meet the deadline. Throughout the process, the new assurances team remained committed to a seamless transition for stakeholders and foreign NSA/DSAs (National Security Authority/Designated Security Authorities).

The new International Assurances branch (IAB) leveraged its fresh perspective of the mission functions and brainstormed new ideas to streamline legacy processes. Specific attention was given to integrating automation into primary mission functions, to ensure processes are performed expeditiously with consistency and accuracy. For instance, solutions developed by the branch include the introduction of an international customer service hotline, e-fax solution, and enhanced metrics for all international assurance products.

Request for Visit (RFV) e-Fax 24/7 Solution

A main task for the branch is processing international outgoing visits for cleared industry. This includes cleared visitors traveling to classified sites or attending classified

ASSUMES ASSURANCE MISSION

By Scott Cronin and Lovely Rodriguez; *Industrial Policy and Programs*

meetings. DSS only processes requests to foreign government facilities or military sites, and NATO locations, but the volume of these visit requests are high. The typical number of annual visit requests is 4,000, which translates to approximately 8,500 visitors to 12,000 destinations.

To address the high volume, as well as the time-sensitive nature of visit requests, IAB introduced an e-fax solution. This automated approach reduces processing time by 15 hours per week, and provides facility security officers with the convenience of submitting RFVs any time, 24 hours a day, 7 days a week, 365 days per year.

In addition, visit requests are received via e-fax and maintained within an IAB group mailbox. These submissions are captured electronically without the need to print a single visit request. DSS estimates this e-file solution will save more than 90,000 pages of paper annually while increasing efficiencies.

Customer Service Client Care

The IAB anticipates processing more than 6,000 assurance actions annually, to include classified outgoing visit requests, foreign facility verification requests, and personal security clearance verifications. The volume of actions opens the door for increased chances for errors. As a way to mitigate the risk for processing error, effective communication is key. IAB has implemented a customer service hotline to enhance communication with industry, sister agencies and foreign NSA/DSAs. A dedicated customer service representative is responsible for fielding calls and providing client care.

Tracking What's Important

Tracking databases are vital to determine the overall volume, consistency and accuracy of the actions IAB processes. IAB has introduced new databases for collecting international assurance metrics and tracks all visit requests.

These databases are instrumental in tracking approximately 8,500 cleared U.S. industry travelers who make classified visits abroad. This includes documenting the names of the visitors, the type and level of classified visits, and pin pointing the final destination of the visits for security accountability to appropriate stakeholders. The new databases have also helped track foreign government requests to verify security clearances for U.S. citizens, within as well as outside the National Industrial Security Program (NISP), who work for foreign companies or foreign governments.

IAB also tracks foreign nationals who have been granted a Limited Access Authorization (LAA), to U.S. Secret classified information. These tracking tools have been a tremendous stride in ensuring personnel security accountability and optimizing performance of IAB actions.

IAB Path Forward

In the future, IAB hopes to utilize automation throughout the visit process, which will reduce administrative error by an estimated 98 percent. IAB also plans to develop an international customer service survey to solicit feedback from stakeholders and foreign NSA/DSAs, in an effort to identify additional areas for improvement and enhance customer satisfaction.

YOU CAN'T SEE ME

WHAT HAPPENED

In July 2012, a cleared contractor's Computer Incident Response Team (CIRT) detected a cleared employee with a Secret personnel security clearance uploading approximately 3,000 files from his company computer to a personal external hard drive.

When questioned a week later, the employee admitted to the file transfer and provided the hard drive to the company for data wiping. A subsequent review of the external hard drive found the drive contained approximately 46,000 files of company data, some of which was company proprietary or sensitive information.

According to the contractor's CIRT, the files appear to have been uploaded on multiple occasions from about June 2010 through July 2012. The employee admitted that some of the files may have been transferred to his personal computer when the hard drive was connected to it at his home.

WHAT WE LEARNED

The employee had been involved in numerous performance incidents at the company dating back several years and had a declining trend in performance evaluations, each of which preceded a file transfer incident. Subsequent to the July 2012 event and the investigation that followed, the company terminated the employee and separated him in the Joint Personnel Adjudication System (JPAS) but did not enter an incident report in JPAS.

In September 2012, the contractor reported the incident to DSS; however, a suspicious contact report (SCR) wasn't written until November 2012 and due to system failure, was not visible until April 2013.

Following the initial incident and the employee's termination, nearly seven months passed before the company submitted an incident report in JPAS. This delay in reporting was due to a glitch in the company's reporting process where the company had completed an internal report of the incident but did not ensure the report's transfer and submission in JPAS. In January 2013, while reviewing the case, the company realized no incident report had been entered and officially submitted a report on the July 2012 incident.

In December 2012, the employee was hired by a government entity. Because the employee's JPAS record reflected current eligibility for access to Secret information and contained no derogatory information, that agency granted the subject access to classified information.

Once DSS discovered the employee had access to classified information without adjudicative visibility of all available derogatory information, DSS forwarded the incident report to the Department of Defense Central Adjudicative Facility (DoD CAF) within 24 hours of receipt.

DoD CAF Industry Division A was unable to take necessary adjudicative actions since another division now owned the subject's clearance. The information was immediately provided to the appropriate division, and after their review, the subject's clearance eligibility was removed by loss of jurisdiction.

RESULTS

This case highlights a vulnerability that went undetected for several months. While the individual in question was hired by a new employer and had access to classified information for one month, a vulnerability persisted for seven months where no potential employer had visibility of an incident involving him. Had the company submitted the report of adverse information in JPAS in July 2012,

and had DSS internal procedures been followed, this vulnerability could have been detected and mitigated months sooner and all necessary adjudicative actions completed in a timely manner.

Upon separation from the organization, the facility security officer (FSO) should enter a separation date for the employee in JPAS. If an investigation is open for the employee, the FSO should send a JPAS notification to the appropriate CAF division to determine whether the investigation needs to be canceled.

Remember: Complete all applicable actions as warranted, including: removing individual access in JPAS, submitting incident reports, and entering separation information. In accordance with paragraph 3-108 of the National Industrial Security Program Operation Manual (NISPOM), contractors must debrief cleared employees at the time of termination of employment (whether by discharge, resignation, or retirement) when an employee's personnel security clearance is terminated, suspended, or revoked, and upon termination of the company's facility clearance.

INCIDENT REPORTING OF ADVERSE INFORMATION IN JPAS

The NISPOM requires that contractors report to DSS any adverse information coming to their attention concerning their cleared employees. Adverse information consists of any information that negatively reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security. Adverse information reports submitted pursuant to NISPOM 1-302a should be recorded as an incident report in JPAS. The JPAS system was designed to accommodate submitting adverse information as an incident report and provides immediate assurance of receipt. JPAS also eliminates the manual handling by multiple individuals when hard copy requests are received and entered into JPAS by adjudication staff.

To facilitate quicker processing of incident reports of adverse information in JPAS, the report must include the basic information covering 'who' (who was involved; for example: subject, law enforcement agency, court name), 'what' (what is/was the incident), 'where' (where did the incident happen; for example: city, state), and 'when' (when did the incident occur).

When submitting an incident report of adverse information in JPAS, refer to the questions on the SF-86 relating to the incident and provide as much information as possible that is readily available.

An adjudicator will review the submitted report and determine if the item may be closed with a new eligibility adjudication entered, or if a partial investigation is required to provide the adjudicator sufficient information to make a decision. After the incident report is reviewed by the adjudicator, the FSO may receive a request for the person to submit a new SF-86. If such a request is made, the FSO should initiate the request to the employee using JPAS. If the request is not received by the DoD CAF within 30 days from the date of request, they will administratively withdraw the eligibility determination by changing the eligibility to Loss of Jurisdiction. At that time, all access must stop.

Sources from which an incident report may be received:
* Facility Security Officers * Other Government Agencies
* Investigative process * Another CAF division's decision to Deny, Revoke or Suspend a (Federal) security clearance *

If there is a question regarding a person having continued access when an incident report is reflected, contact the DoD Security Services Center at 888-282-7682 for assistance.

TRAINING AVAILABLE

The Center for Development of Security Excellence provides a 30 minute webinar on Adverse Information Reporting. The webinar is designed to provide an understanding of reporting responsibilities under NISPOM 1-302a and ISL 2011-04, what types of information that should be reported, how to make reports, and where to send reports. Access the webinar at www.cdse.edu/catalog/webinars/industrial-security/adverse-information-reporting.html.

WHAT IS THE **NITT**? WHAT IS **INSIDER THREAT**?

HOW DOES IT AFFECT THE **NISP**?

By Lisa Gearhart
Industrial Policy and Programs

As a result of the WikiLeaks release of thousands of classified documents through the global media and internet, Executive Order (E.O.) 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing of Classified Information,” was signed October 7, 2011.

The executive order established the National Insider Threat Task Force (NITTF) to help prevent another WikiLeaks-type incident, or the unauthorized disclosure of classified information through espionage through a national insider threat policy, with supporting standards and guidance.

The NITTF is co-chaired by the U.S. Attorney General and the Director of National Intelligence (DNI). They, in turn, designated the Federal Bureau of Investigation and the National Counterintelligence Executive to co-direct the daily activities of the task force.

The NITTF was tasked to:

- Develop a government-wide policy and minimum standards for deterring, detecting, and mitigating insider threats
- Includes safeguarding classified information from exploitation, compromise or unauthorized disclosure
- Provide assistance to agencies, as requested
- Provide analysis of insider threat challenges facing the United States government

On November 21, 2012, Presidential Memorandum, “National Insider Threat Policy and Minimum Standards for Executive Branch Threat Programs,” was issued. It gave executive departments and agencies 180 days to:

- Establish a program for deterring, detecting and mitigating the insider threat
- Designate a senior official(s) with the authority to provide management, accountability and oversight of the organization’s insider threat program and make resource recommendations to the appropriate agency official

The National policy applies to “… contractors and others who access classified information, or operate or access classified computer networks controlled by the federal government…”

What is an insider threat? It is a threat posed to U.S. national security by someone who has authorized access to classified or national security-related information but who misuses or betrays that access by providing it to an entity not authorized to possess it, such as a foreign government, an individual, or even the media.

How will insider threat affect the National Industrial Security Program (NISP)? Title 32 Code of Federal Regulation (CFR) 2004, NISP Implementing Directive, is being revised to incorporate insider threat responsibilities for the cognizant security agencies (CSAs) and the government contracting activities. The CSAs include the Department of Defense, Department of Energy, Nuclear Regulatory Commission and the DNI.

Additionally, the DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), is being revised to include insider threat requirements.

The NITTF has developed training related to insider threat. The training includes:

- **“Establishing and Operating an Insider Threat Program”** and **“Principles of a Hub Operation.”** Additional information can be found at: www.ncix.gov

In addition, the DSS Center for Development of Security Excellence (CDSE) has developed the following insider threat training:

- **“Insider Threat Awareness, CI121.06.”** Additional information can be found at: www.cdse.edu/catalog/elearning/CI121.html

- **“Establishing an Insider Threat Program for Your Organization, CI122.16.”** Additional information can be found at: www.cdse.edu/stepp/index.html listed within the Counterintelligence, eLearning section

>> COMMUNICATION OF THE FUTURE

OFFICE OF THE CHIEF INFORMATION OFFICER BUILDS A COLLABORATIVE NETWORK ACROSS DSS

By Luis Garcia
Office of the Chief Information Officer

Network convergence is the concept of combining voice, video, fax, data and other signal transmissions into an efficient single high-speed network infrastructure. While not a new concept, it is new to DSS, and five field offices are slated to participate in a pilot program in January 2014.

This concept, when deployed correctly, results in great economic benefit. Some of the specific benefits include: reducing costs of maintaining/securing multiple networks, reducing costs of multiple circuits through scaling, combination of services/applications in one media and mobility.

Network convergence has been around for several decades, but for the past 10 years, general advances on the internet, quality of service and the high use of IP-based protocols provide DSS with the perfect environment to support implementation of convergent networks. This is a new capability for DSS, and it will provide the foundation for the next-generation enterprise communications.

A converged network platform will provide DSS with a "private cloud" that operates at a lower cost with higher performance and built-in redundancy. At an average cost of approximately $8,000 per site, the Office of the Chief Information Officer (OCIO) can reuse current hardware when re-engineering the infrastructure to meet DSS mission goals. Strategic investment like this will pay for itself in less than 12 months. Additional savings will be achieved by freeing long distance calls, reducing hardware maintenance costs, consolidating telecommunications contracts and reducing data circuit costs.

THIS NEW NETWORK ENTERPRISE ... CAN SIGNIFICANTLY ENHANCE IT CAPABILITIES AND COMMUNICATIONS SECURITY

Currently, five field offices have been chosen to take part in the pilot project. Offices have been chosen based on their geographic separation to ensure an accurate proof of concept. Starting in January 2014, Atlanta, Tacoma, Linthicum, San Antonio and Phoenix will be connected to this new enterprise infrastructure while maintaining their existing connection.

Feedback from the offices is vital to help prove the concept and provide lessons learned. This new network enterprise approach will not only be economically attractive but can significantly enhance IT capabilities and communications security provided to the field.

Integrating voice, video and data with the computer desktop/laptop applications will enhance and facilitate real time communications among field offices and industry. Services include voicemail or a fax that can be easily redirected to a user's email account during a site visit to industry. The service provides the capability to launch a live video session on the desktop, enhanes communication between field offices and industry, and allows collaboration on projects as if participants were in the same room. These examples are just a few of many benefits a unified communication network can provide.

THE IMPORTANCE OF USING MULTIPLE SOURCES IN INTELLIGENCE AND INVESTIGATIONS

By Jeremiah Anderson
Counterintelligence Directorate

History shows us that striking a balance between protecting the critical information/technology comprising the U.S. industrial base and bringing to justice those accused of espionage is a delicate process. This process is especially difficult in cases motivated by ideology because of the lack of the usual indicators. Once more information becomes available later, it sometimes becomes evident that investigators struck this balance incorrectly.

Additionally, using multiple intelligence sources in developing cases for investigation and prosecution is critical, as performing hasty analyses based on limited information greatly increases the probability of an erroneous assessment.

Corroboration of information is also important, not just because it improves the accuracy of an assessment but because it may lead to a lower classification of the information, thus allowing for wider dissemination.

The government must also be willing to publicly disclose ways and means in court during an espionage case, further reinforcing the importance of corroborating intelligence of low classification.

An example of the government's failure to use multiple sources to verify highly classified intelligence is the Rosenberg spy case of the 1940s-'50s. However, it was an incredible stroke of luck that the Rosenbergs' activities were discovered at all: they exhibited no indicators of espionage and might have gone undetected indefinitely — save for an Army cryptographic program named VENONA.

VENONA was the code name for the U.S. Army Signal Intelligence Service's decryption of Soviet diplomatic cables sent from Soviet missions in the United States to Moscow. Beginning in February 1943, VENONA project personnel worked to break the KGB encryption and were largely successful in doing so by 1945.

However, the decryption process was extremely time-consuming: the Army could not read Soviet messages until two years after they had been sent. Nonetheless, by 1948 enough messages had been decrypted to begin an investigation into Soviet espionage on the Manhattan Project, the U.S. effort to develop an atomic bomb.

The FBI worked with VENONA personnel to identify targeted individuals, locations, and programs mentioned in Soviet diplomatic correspondence using codenames. The FBI provided VENONA personnel with a list of over 200 KGB code names, and with this information the VENONA team was able to narrow the list of people for the FBI.

In August 1949, the FBI identified Klaus Fuchs as the first in a series of spies. Fuchs had fled Nazi Germany and became a British scientist assigned to the Manhattan Project. However, because

LEFT: Klaus Fuch's Los Alamos ID badge photo. *U.S. Department of Energy.* **RIGHT:** Julius and Ethel Rosenberg, separated by heavy wire screen as they leave court after being found guilty by a jury. *New York World-Telegram & Sun; Library of Congress.*

of the extreme secrecy of VENONA, the Bureau could not use the intercepted Soviet communiqués to charge Fuchs.

Instead, the FBI was able to secure a confession from Fuchs in 1950 using other information gleaned from VENONA. Fuchs's confession led the FBI to other individuals engaged in espionage, culminating in the arrests of Julius and Ethel Rosenberg. The Rosenbergs never had direct access to the information they passed to the Soviets. Rather, Julius recruited several individuals who worked within the Manhattan Project, and both he and Ethel acted as intermediaries between the recruited spies and the Soviets.

In March 1951, the Rosenbergs were put on trial for conspiracy to commit espionage. In an effort to direct the investigation toward others working for the Soviets, the FBI pressured the Rosenbergs to confess their activities; however, neither did so.

Unable to present Soviet intercepts in court because that would have compromised VENONA, the prosecution relied on the Rosenbergs' communist affiliation and testimony from Ethel's brother to secure a conviction. On June 19, 1953, they became the only Americans ever executed for espionage during peacetime.

Despite VENONA's success, the inability to corroborate information gathered from Soviet intercepts via multiple additional sources produced unfortunate consequences. When VENONA documents pertaining to the Rosenbergs were declassified in 1995, they revealed that several individuals, to include Theodore Hall and Saville Sax, had escaped prosecution.

By the time the FBI was alerted to these espionage activities, years had passed, and the FBI was unable to prove these individuals had passed information to the Soviets. As with the Rosenbergs, the FBI had no other sources with which to corroborate intelligence gathered through VENONA and could not risk divulging the intercepts in court. Hall and Sax continued to live in the United States until their deaths, never charged with espionage.

Furthermore, upon viewing the declassified VENONA documents, it became evident that Ethel Rosenberg had played a minor role in facilitating Julius' espionage activities, and Ethel was convicted and executed on the basis of inaccurate evidence.

Using multiple sources in investigations and analysis is critically important for ascertaining the whole picture so that end users of intelligence can make proper decisions. Had multiple sources been used, Theodore Hall and Saville Sax may well have been brought to justice and Ethel Rosenberg might not have been executed — and a much fuller picture of Soviet espionage in the United States might have ultimately been discerned.

TOASTMASTERS INTERNATIONAL®

FIVE SHIELDS TOASTMASTERS

Club 3258313

Quantico, Virginia

A "MID-WEEK OASIS"

TOASTMASTERS COMES TO RKB!

In late September, several DSS employees participated in the chartering ceremony for the new Five Shields Toastmasters Club — an organization open to the Russell-Knox Building (RKB) community.

Toastmasters International is comprised of 14,350 clubs in 122 countries, with a membership of 292,000 people. The mission of Toastmasters is to empower individuals to become more effective communicators and leaders, and its vision is to become a first-choice provider of dynamic, high-value, experiential communication and leadership skills development.

A Toastmasters meeting is a learn-by-doing workshop in which participants hone their speaking and leadership skills in a no-pressure atmosphere. There is no instructor; instead, members evaluate one another's presentations and the feedback process is a large part of the program's success.

The September ceremony marked the end of a journey which started over a year ago. Gerald Curry, chief of staff, Industrial Security Field Operations (ISFO), and long-time Toastmaster, started the process for establishing a club in June 2012. With the approval of the Marine Corps Base Quantico commander, the club attained the required membership to be chartered by Toastmasters International shortly thereafter. The first regular club meeting was held in July 2012, and regular weekly meetings have been held since. The chartering ceremony marked the official presentation of the club's charter from Toastmasters International.

The Five Shields Toastmasters is open to employees of all agencies and companies operating within RKB, but DSS employees play a particularly prominent role. Curry is the club's official sponsor and serves as the vice president for membership. Dana Richard, Counterintelligence, is the club's president; Kim Colon, Strategic Management Office, is the vice president for education; Deborah Keefe, Industrial Policy and Programs, is the assistant sergeant at arms; Adriane Johns, ISFO, assists in membership; and defense contractor Jovella Barnett assists the secretary.

During the ceremony, Richard articulated a vision for the club to serve the needs and interests of the club's three audiences — its members, the RKB agencies and companies who employ them, and the Toastmasters International organization.

In his remarks, Richard emphasized that Toastmasters can be of benefit to members regardless of their previous level of experience.

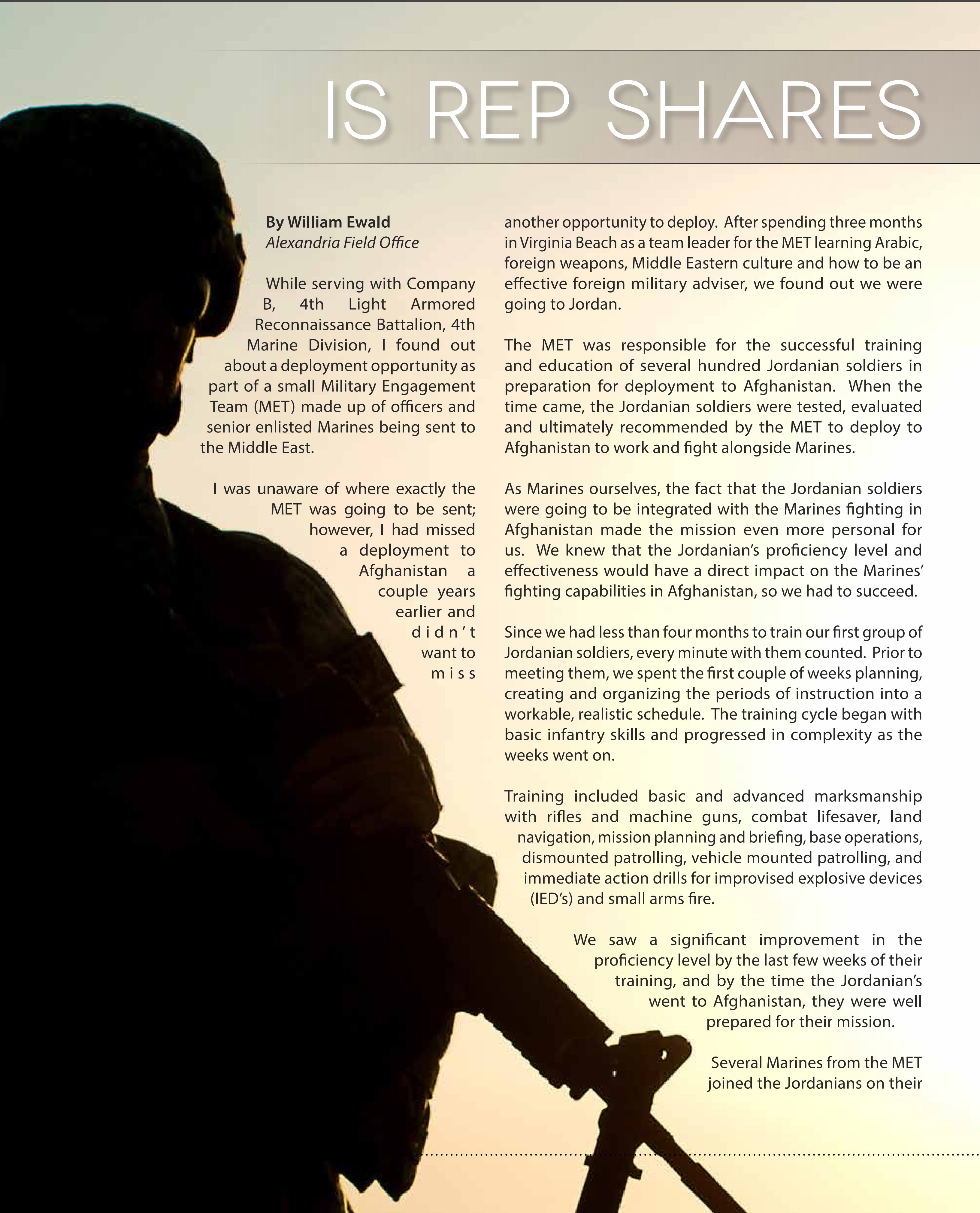
"Members who have little or no public speaking experience and training can develop basic skills, while experienced speakers can hone and refine skills required for higher levels of achievement," he said.

"And being a Five Shields Toastmaster also enhances productivity by being a 'mid-week oasis' where members can recharge during busy work weeks."

The Five Shields Toastmasters envisions:

- Becoming a recognized venue for professional development by the RKB agencies;
- Becoming a center for personal growth and professional development for the personnel who work within RKB;
- Maintaining a member-centric focus in which:
  1. The club is a mid-week oasis for the RKB workforce;
  2. Every Toastmaster within RKB is enabled to achieve their personal and professional goals; and
  3. The club is a safe, nurturing, and challenging environment for personal growth and achievement.

TOP LEFT: Gerald Curry, Industrial Security Field Operations chief of staff and official sponsor of Five Shields Toastmasters, makes introductions at the start of a meeting. **TOP RIGHT:** Carolyn Lyle, Equal Employment Opportunity chief and member of Five Shields, hones her speaking skills.



IS REP SHARES

By William Ewald
Alexandria Field Office

While serving with Company B, 4th Light Armored Reconnaissance Battalion, 4th Marine Division, I found out about a deployment opportunity as part of a small Military Engagement Team (MET) made up of officers and senior enlisted Marines being sent to the Middle East.

I was unaware of where exactly the MET was going to be sent; however, I had missed a deployment to Afghanistan a couple years earlier and didn't want to miss another opportunity to deploy. After spending three months in Virginia Beach as a team leader for the MET learning Arabic, foreign weapons, Middle Eastern culture and how to be an effective foreign military adviser, we found out we were going to Jordan.

The MET was responsible for the successful training and education of several hundred Jordanian soldiers in preparation for deployment to Afghanistan. When the time came, the Jordanian soldiers were tested, evaluated and ultimately recommended by the MET to deploy to Afghanistan to work and fight alongside Marines.

As Marines ourselves, the fact that the Jordanian soldiers were going to be integrated with the Marines fighting in Afghanistan made the mission even more personal for us. We knew that the Jordanian's proficiency level and effectiveness would have a direct impact on the Marines' fighting capabilities in Afghanistan, so we had to succeed.

Since we had less than four months to train our first group of Jordanian soldiers, every minute with them counted. Prior to meeting them, we spent the first couple of weeks planning, creating and organizing the periods of instruction into a workable, realistic schedule. The training cycle began with basic infantry skills and progressed in complexity as the weeks went on.

Training included basic and advanced marksmanship with rifles and machine guns, combat lifesaver, land navigation, mission planning and briefing, base operations, dismounted patrolling, vehicle mounted patrolling, and immediate action drills for improvised explosive devices (IED's) and small arms fire.

We saw a significant improvement in the proficiency level by the last few weeks of their training, and by the time the Jordanian's went to Afghanistan, they were well prepared for their mission.

Several Marines from the MET joined the Jordanians on their movement to Afghanistan to serve as a liaison between the Jordanian soldiers and Marines they were attached to. After several weeks of fusing the two forces together, the Marines from the MET returned from Afghanistan with nothing but positive remarks about the Jordanians in their first few weeks in country. This meant a lot to us, as every Marine put maximum effort and a personal commitment into the mission.

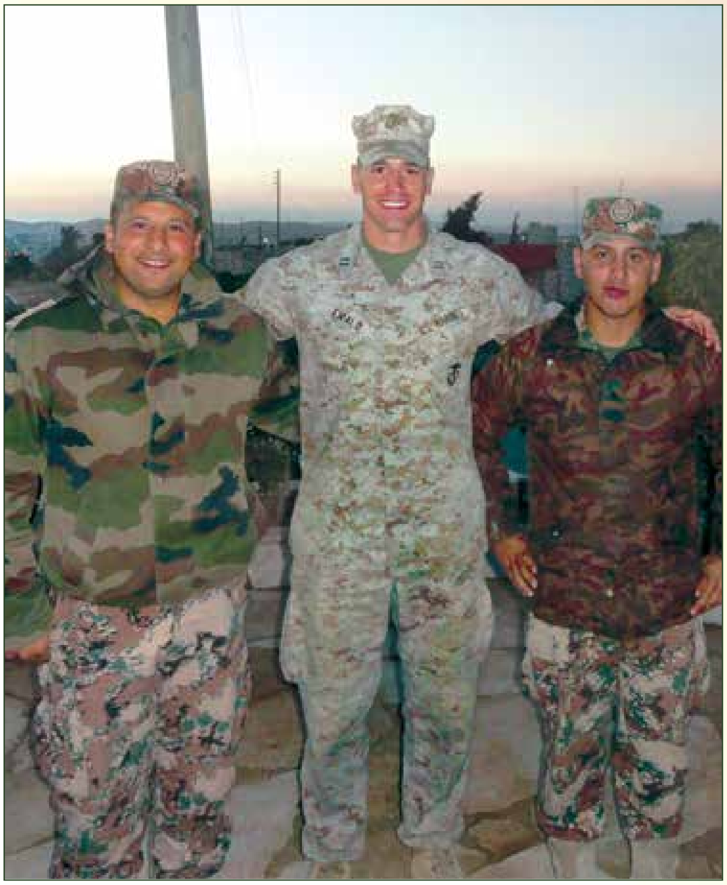
Although the primary mission was to train the Jordanians for combat operations, we were able to squeeze some time in for our own training as well. We conducted our own rifle ranges, physical training, martial arts training, and professional military education, continuously refining the skills and abilities required of Marines.

As Marines, and America's first responders, we prided ourselves on our ability to carry out any mission at any time. With today's uncertainties in the Middle East, it was more important than ever that we stayed fully mission capable and ready to handle anything that may have come our way.

The professional and personal experiences gained by the Marines over the course of the seven month deployment to Jordan could not have been better. I know that I, and each Marine on the MET, learned a lot about each other and themselves as well.

These experiences, like ours, from individual Marines stationed all over the world are what shape the Marine Corps into the versatile and highly effective group of warriors it is today.

With all of the exciting and new experiences I had over the course of the seven month deployment, however, for me, nothing can compare to the feeling of setting foot back on American soil and seeing the American flag waving in the wind.



AT RIGHT: William Ewald (center), industrial security representative in the Alexandria 1 Field Office and a captain in the U.S. Marine Corps Reserves, congratulates two officers in the Jordanian military for completing their training.

William Ewald is an IS rep in the Alexandria 1 Field Office and has been with DSS since January 2011. He was commissioned in the U.S. Marine Corps Reserve in December 2008 and after completing Infantry Officer Course in 2009, served three years as an infantry platoon commander and the executive officer for Bravo Company, 4th Light Armored Reconnaissance Battalion, Frederick, Md.

He was activated for deployment in October 2012, serving as a company team leader for the Military Engagement Team – Jordan. He is currently a captain and a student in the U.S. Marine Corps Expeditionary Warfare School.

RECOGNIZING EXEMPLARY CI WORK

In August 2013, Greg Topczewski, security manager, Navigation & Maritime Systems Division (NMSD), Northrop Grumman System Corporation, Charlottesville, Va., was presented with a certificate of appreciation by the Virginia Beach Field Office for his counterintelligence efforts.

Specifically, Topczewski was honored for his exemplary work, leadership and achievements in the area of suspicious contact reporting as it relates to Northrop Grumman System Corporation's counterintelligence integration efforts in identifying multiple individuals attempting to penetrate the cleared contractor's performance on classified contracts within the National Industrial Security Program.

Pictured (from left) are: Jeff Holloway, site manager, Maritime Systems; Bruce Rainey, field counterintelligence specialist; Greg Topczewski, security manager, NMSD; Beth Whatley, field office chief; Andrae Walker, senior industrial security specialist; and Linda Hansen, security director, NMSD.

WORKING GROUP MEETS, UPDATES ISOM MODULE 17

Industrial Security Field Operations (ISFO) hosted field supervisors and an industrial security representative in August 2013 at DSS headquarters, Quantico, Va., to revise and update Module 17 of the Industrial Security Operating Manual.

Module 17 defines the duties of a field office chief as they relate to establishing supervisory roles and responsibilities, administrative duties, span of control, field office management and best practices. This working group was chartered in early 2013 to revise and update internal processes and procedures, and to create a guide for newly hired supervisors.

The attendees were from all four regional (Capital, Northern, Southern, Western) areas of operation. Participants from the Northern Region were Heather Sims (St. Louis Field Office), Gary Sims (St. Louis Field Office Team Lead), Donna Walker (Detroit Field Office), John Donnelly (Andover Field Office) and Salvatore Urbano, (ISR- St. Louis).

Participants from the Southern Region were Jennifer Norden (Irving Field Office) and Beth Whatley (Virginia Beach Field Office). Matthew Roche (Alexandria Field Office) represented the Capital Region, Norman O'Brien (Sunnyvale Field

Office) represented the Western Region, and Adriane Johns, represented DSS Field Operations Headquarters.

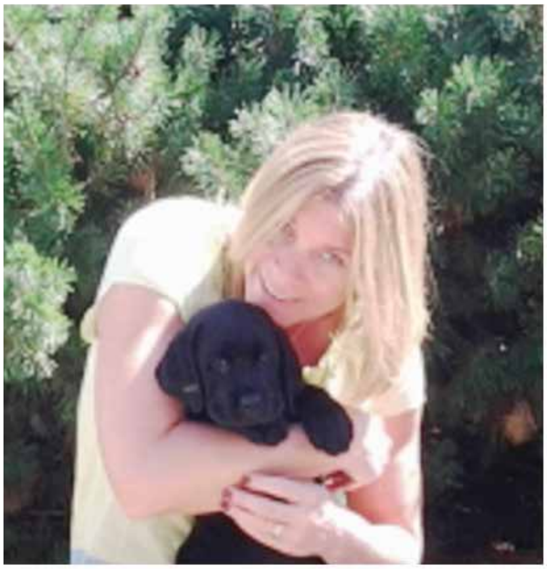
The meeting agenda focused on determining baseline requirements, assignment of tasks, and documenting processes. Through discussions, the team discovered "best practices" which had been adopted by some offices, with plans to incorporate these processes into the final plan.

The meetings also provided supervisors an opportunity to meet face-to-face with their counterparts, which facilitated a productive exchange of ideas and information. The work of the group built upon previous efforts to standardize the role and responsibilities of the field office chief.

"The goal of the group is to provide a useful tool for all field supervisors, instead of a requirements document," said Johns. "Additionally, the team is creating an interactive webpage to provide one-stop shop for commonly used documents, sharing lessons learned, and developing tools to prepare future field supervisors."

The working group will continue to meet and produce a final product that will be socialized across the field. They plan to deliver a final product for review by first quarter of the new fiscal year.

SERVICE DOG NAMED FOR PRESTIGIOUS AWARD



At the June 2013 training seminar, NCMS requested contributions in support of "America's Vetdogs" and raised $7,950. The not-for-profit organization, founded by the accredited Guide Dog Foundation for the Blind, serves disabled veterans and active duty personnel.

In recognition of the generous support, America's Vetdogs honored NCMS by allowing the organization to name one of its puppies! NCMS Board Member and Seminar Chair Aprille Abbott picked the puppy, and based on an overwhelming vote by the NCMS Board, named him "Cogswell."

FIELD OFFICE BUILDS PARTNERSHIP THROUGH RIDE-ALONGS

By Nicole Graham
Office of Public and Legislative Affairs

"A ride-along is another way to tell the DSS story," said Sharon Dondlinger, the Alexandria-2 Field Office chief. Dondlinger has embraced the ride-along model and forged relationships with government customers at the same time. As Dondlinger notes, "security is our mission, and no other agency solely has that mission."

It was through training and conferences that Dondlinger met and reconnected with industrial security officials from other government agencies. Monica Dempsey of the Air Force District of Washington (AFDW) was one such contact who became interested in the DSS mission during a training event.

In April, the Alexandria Field Offices hosted eight AFDW participants for a briefing on how DSS supports Air Force contracts. During the briefing Dondlinger, Matthew Roche, Alexandria-1 Field Office chief, and Industrial Security Specialist (ISS) Grant Ward provided AFDW with an overview of DSS, discussed the agency's capabilities, and answered questions.

Since the Air Force has an established industrial security function, they were more interested in learning how other agencies operate. In order to give them a hands-on experience, AFDW was invited to ride along during two assessments of cleared facilities with U.S. Air Force contracts.

During the ride-along, AFDW wanted to gain an understanding of how DSS operated on such a large scale in order for them to expand investigations into their contracts. DSS representatives shared what they did, what they looked at, and discussed the security procedures and steps DSS takes during an on-site assessment.

The ride-along also provided DSS with an opportunity to demonstrate the implementation of the updated vulnerability assessment ratings matrix. The Air Force team liked that the rating matrix explained National Industrial Security Program (NISP) enhancements and vulnerabilities while creating a fair and tangible process. Furthermore, they believed the measurable results showed companies what they must strive for to be the best in security and believe a similar tool would be useful on their end.

Additional Interagency Partnerships

The Information Security Oversight Office (ISOO) is the part of the executive branch that oversees the NISP and the government-wide security classification system. In order to ensure the National Industrial Security Program Operating Manual is being sufficiently implemented, ISOO occasionally joins ride-alongs with DSS personnel to cleared facilities. In the past year, ISOO personnel have accompanied the Alexandria-2 Field Office on two occasions.

ISOO has expressed interest in conducting assessments of government agencies to ensure they are properly marking and implementing the correct classification guidance, and determining whether the government is effectively providing industry with sufficient tools to maintain this requirement. Therefore, these ride-alongs are extremely convenient for ISOO since they are not only able to watch what DSS is doing but also what the cleared contractors are doing. Ward, who participated in the ride-along with ISOO, said the ride-along was very productive and was a great way to gain another perspective on how assessments are completed.

The Alexandria-2 Field Office is also developing a partnership with the National Guard Bureau (NGB). In the fall, NGB received the same briefing as AFDW, and joined a ride-along. The NGB wanted to know more about the handling of classified information and was interested in guidance to implement security procedures when dealing with its contractors.

Dondlinger stated, "Ride-alongs are a great way to develop relationships with other agencies. Not only are the ride-alongs educational, but they encourage interagency collaboration." In the future, Navy industrial security representatives from Patuxent River Naval Air Station, Md., intend to participate in a DSS ride-along.

A Way to Share the DSS Story

Personnel from across DSS can also join the ride-alongs. As Ward noted, ride-alongs "provide other departments the ability to experience different situations DSS will come across during an assessment." The increased interaction between the directorates helps to demonstrate, through first-hand experience, how the field is implementing industrial security procedures. Feedback allows DSS to develop new policies to make the industrial security process as effective as possible.

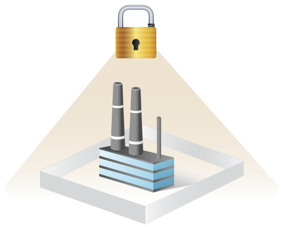
Ride-alongs have been very successful and supportive of DSS operations. These joint exercises help field offices establish points of contact at government agencies and cleared facilities. The relationships built through these ride-alongs can prevent or quickly resolve issues that occur at facilities under the purview of DSS.

FY13 | DSS BY THE NUMBERS

13,321 active, cleared facilities in the National Industrial Security Program (NISP)

CLEAR AND ASSESS FACILITIES

- 7,096 Vulnerability Assessments
- 1,285 New facility clearances granted
- 15,000 Accredited systems in industry
- 26 Federal Partners in addition to DoD Activities



PERSONNEL SECURITY MANAGEMENT OFFICE FOR INDUSTRY (PSMO-I)

- 172,499 PSI Submissions for Industry FY13

FUND NISP PERSONNEL SECURITY INVESTIGATIONS

- Estimated $214 million expended overall in FY13

PERFORM COUNTERINTELLIGENCE (CI) FUNCTIONS

- 31,646 Reports of suspicious contact from Industry
- 6,277 DSS referrals to LE/IC
- 717 Investigations/operations opened due to DSS reporting
- 3,472 Intelligence Information Reports
- 3,291 Personnel attending seven CI Webinar events

MITIGATE FOREIGN OWNERSHIP CONTROL OR INFLUENCE (FOCI) IN CLEARED INDUSTRY

- 732 FOCI facilities
- 337 FOCI mitigation agreements
- 68 FOCI agreements emplaced FY13

IDENTIFY/MITIGATE THREATS AND VULNERABILITIES IN NISP

- 642 Total cases reviewed in FY13*
- 506 Vulnerabilities identified** (78.8% of all OAG cases)
- 429 Identified vulnerabilities mitigated (84.7%)
- 20.5 Days to mitigate vulnerability (average)
- 184 PCL actions taken
- 58 FCL actions taken

CDSE CORE CERTIFICATION PROGRAM***

- Security Fundamentals Professional Certification (SFPC)
  3,994 Total Candidates Tested/1,817 Conferrals
- Security Asset Protection Professional Certification (SAPPC)
  670 Total Candidates Tested/425 Conferrals
- Security Program Integration
  284 Total Candidates Tested/164 Conferrals
- Adjudicator Certification
  622 Total candidates Tested/535 Conferrals

* Information reviewed by information received from our field elements, government partners, or open source media.
** A condition in the industrial security program, facility security procedures, internal DSS controls, implementation, or lack of conformance to procedures that could be exploited or triggered by a source that places U.S. technologies at risk.
*** Note: Conferrals include Beta and Honorary totals

DEFENSE SECURITY SERVICE