DSS ACCESS

VOLUME 2, ISSUE 2

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE

ANNUAL FOCI CONFERENCE

BRINGS EXPERTS TOGETHER

SUMMER 2013

VOLUME 2, ISSUE 2

DSS ACCESS

Published by the
Defense Security Service
Public Affairs Office

27130 Telegraph Rd.
Quantico, VA 22134
dsspa@dss.mil
(571) 305-6751/6752

DSS Leadership

Director
Stanley L. Sims

Deputy Director
James J. Kren

Chief of Staff
Rebecca J. Allen

Chief, Public Affairs
Cindy McGovern

Editor
Elizabeth Alber

Graphics
Steph Struthers

DSS ACCESS is an authorized agency information publication, published for employees of the Defense Security Service and members of the defense security and intelligence communities.

FROM THE DIRECTOR

The saying, "May you live in interesting times" is widely reported to be of ancient Chinese origin and is considered a curse rather than a blessing. While I'm not qualified to comment on the origin of the saying, but I think I can say with some certainty that these are truly interesting times in which to live and serve. I also think 'interesting times' provide unique opportunities, which I am proud to say, DSS has embraced.

This issue of ACCESS highlights some of the creative and innovative solutions DSS employees have developed to better meet the agency mission and support the members of the National Industrial Security Program in these interesting times. We have the San Antonio Field Office hosting a 'Day with DSS,' which is designed to foster outreach to the cleared facilities in their area. The Hanover Field Office started their own diversity program to provide training opportunities to employees who are unable to travel to the headquarters to attend programs.

The Capital Region's Counterintelligence folks initiated a partnership with the local FBI office that has led to an enhanced working relationship and better support to their cleared contractors. And the Center for Development of Security Excellence established a contract with a commercial testing firm to ensure that certification testing is available worldwide.

Each of these initiatives was a grass-roots effort generated by a motivated workforce. In each case, a DSS employee or office recognized a need and, leading by example, made a difference. I didn't come up with these ideas, I just get to take the credit and share them with our readers! I want to emphasize that these are just a few of the examples of the great work going on in DSS.

I often tell the DSS workforce to continue to focus on the mission and not let the larger political issues of the day affect our ability to do our jobs. I like to think that message is resonating and this issue of ACCESS makes that clear.

ANNUAL FOCI CONFERENCE BRINGS EXPERTS TOGETHER

By Stefanie Valero
Industrial Policy and Programs

The Defense Security Service (DSS) held its annual Foreign Ownership, Control, or Influence (FOCI) Conference in March at the MITRE facility in McLean, Va.

The two-day conference helped educate the Outside Director, Proxy Holder, and facility security officer (FSO) communities on current DSS- and FOCI-related concerns. It also acted as a forum for contractor input regarding the implementation of FOCI mitigation and operations of security oversight programs. The first day of the conference was specifically designed for Outside Directors and Proxy Holders, while the second day was dedicated to FSOs.

Approximately 350 Outside Directors, Proxy Holders, and FSOs attended the annual event, which has been held 17 times since 1989. The event originally hosted only Outside Directors and Proxy Holders. In 2010, DSS hosted the first FSO conference, and based on the overwhelmingly positive feedback, DSS committed to continue FSO involvement during the annual events.

Both days of the conference started with a welcome from DSS Director Stan Sims, who presented an overview of the current state of DSS. Sims also gave his vision for the future of the agency in an ever-changing security environment.

He mentioned strengthening partnerships between the U.S. government and industry while seeking opportunities to empower the Government Security Committees of FOCI-mitigated companies.

During the afternoon of the first day, J.C. Dodson, vice president of information security for BAE, presented BAE's global cyber security program called "In the FOCI Environment." BAE is a FOCI company.

On a similar theme, Douglas Bruns, technical director for BAE Global Security Operations Center, gave a "Reality Bytes" presentation to the FSOs, on inside global cyber security operations. Both BAE representatives portrayed a partnership between several large defense contractors battling cyber threats to protect sensitive proprietary data on unclassified networks and U.S. national security.

The industry representatives deemed this information insightful since competitive environments usually prevent

CLOCKWISE FROM TOP LEFT:

J.C. Dodson, vice president of information security for BAE, gives a presentation on BAE's global cyber security program called "In the FOCI Environment."

Steve Lewis, Office of the Under Secretary of Defense for Intelligence, listens to the presentations.

The **Honorable William Lynn**, former Deputy Secretary of Defense and current chief executive officer/president of DRS Technologies, Inc., provides the keynote address.

Ben Richardson, chief of the DSS FOCI Operations Division, provides an update on FOCI.

collaborative relationships between companies that the BAE representatives promoted.

On the second day of the conference, the Honorable William Lynn, former Deputy Secretary of Defense and current chief executive officer/president of DRS Technologies, Inc., another company with a FOCI mitigation agreement, provided the keynote address to the FSOs.

His presentation included a discussion on his experiences within the Department of Defense (DoD), industry, and on Capitol Hill, as well as his perspectives on foreign investment in the defense industrial base and the current climate of DoD in the globalized market.

Aimen Mir, staff chair and director, Committee on Foreign Investment in the United States (CFIUS), Office of Investment Security, U.S. Department of Treasury, also spoke and provided a background and overview of current CFIUS procedures. Joanne Isham, former deputy director for Science and Technology at the Central Intelligence Agency, and current Outside Director and Proxy Holder, and The Honorable Stephen Cambone, former Under Secretary of Defense for Intelligence and current Proxy Holder, conducted a panel discussion.

They answered questions from the audience regarding the relationship between FSOs and Outside Directors/ Proxy Holders as well as their relationship with the associated foreign parent companies. The panel discussion also focused on the additional roles and challenges that FSOs encounter at companies operating under FOCI mitigation agreements.

Throughout the conference DSS subject matter experts provided updates on other topics including FOCI oversight, cybersecurity, and Counterintelligence. At the conclusion of activities on both days, a panel of DSS experts fielded questions from the audience.

FROM TOP:

DSS employee **Richard Stahl**, chief of the International Division fields questions from the audience.

DSS **Director Stan Sims** welcomes attendees to the Foreign Ownership, Control, or Influence (FOCI) Conference and presents an overview of the current state of the DSS.

Photos by Derik Bland

For more information regarding the DSS FOCI program, please visit: www.dss.mil/isp/foci/foci_info.html.

DSS RECOGNIZES

EMPLOYEE, TEAM OF THE YEAR

At the 2nd annual Director Awards Ceremony in February 2013, DSS Director Stan Sims recognized the recipients of the DSS Employee of the Year and DSS Team of the Year awards.

David Scott, Industrial Security Field Operations, was named 2012 Employee of the Year and the Operations Analysis Group was named the 2012 Team of the Year.

The Director Awards program recognizes those who exhibit the highest standards of excellence, dedication, and accomplishment in advancing the agency's mission. "We established the Director Awards to shine the light on great work," Mr. Sims said at the ceremony. "The award ensures your dedication to the mission does not go unnoticed."

Sims noted that all employees who were nominated — whether they won or not — were already winners. "You have already been recognized by either a colleague or a supervisor for making a difference," he said. "Each nominee made a significant impact on DSS and the advancement of its mission and I applaud all of you."

In recognizing David Scott, Sims noted, "This year, we started to take on the new mission, with no additional resources, of performing Command Cyber Readiness Inspections (CCRI). After we took on the mission, David developed and drafted a process guide outlining the methodology for the inspections.

"He also suggested we do pre-inspections to help prepare industry for the inspections," Sims added. "Since DSS started doing pre-inspections, we have not had any company fail their CCRI. That's because of the initiative of folks like David. He figured out how to do this mission the right way."

Scott, a senior information system security professional with the Office of Designated Approving Authority, was nominated for program improvements associated with the DSS CCRI process. In particular, Scott's nomination package cited, "David's initiatives to enhance the process of preparing contractor sites for CCRI have significantly advanced the DSS CCRI program, which improved contractor site inspection results and the security posture of the DoD global information grid."

Additionally, "David authored and implemented a secure internet protocol (SIPRNet) Connection Approval Process guide for contractor sites that received rave reviews from the authorities responsible for the SIPRNet connection approval process across DoD.

"As a result of David's initiatives, SIPRNet oversight and preparation for CCRIs has significantly improved over the

course of the year. CCRI outcomes are now revolutionary and day-to-day oversight substantially increased."

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

"In the beginning, the OAG was a fledgling organization with only one permanent employee," Sims said at the ceremony. "The rest of the staff was on temporary loan from their directorates. But once there was a standard operating procedure in place and the OAG concept started showing results, I decided it needed more structure and resources. Now we have a core group of individuals assigned to the OAG that are augmented by other offices across the agency.

"If you look at the numbers, the OAG had a stellar year in 2012 and worked hard to drill down to determine systemic issues and address them," the Director continued.

In its nomination package, the OAG was cited for establishing partnerships that integrated both service delivery and policy to better serve internal and external customers; and innovation in identifying and addressing agency-wide systemic issues. Additionally, the OAG established the first agency-wide concept of operations. DSS business units now have a plan available designed to address and resolve internal/external vulnerabilities.

As a part of those efforts, the OAG reviewed 590 cases in 2012; a 375 percent increase from the OAG's inception in FY10. This resulted in the identification of 120 internal (DSS) and 118 external vulnerabilities, with resolution of 220. These actions, said the nomination — exceeded the expected performance, led cross directorate operations and intelligence integration, identified and stopped threats to and vulnerabilities within the cleared industrial base, and implemented numerous systemic fixes."

This year, a change was made in the nominations for the Employee of the Year award. Previously, only those individuals who were named Employees of the Quarter could compete for the Employee of the Year award. This year nominations for the Employee of the Year Award were open to all DSS employees.

LEFT: Members of the Operations Analysis Group hold their plaques for winning the 2012 Team of the Year Award.

ABOVE: David Scott (left), Industrial Security Field Operations, receives the plaque from DSS Director Stan Sims for being named 2012 Employee of the Year Award.

2012 Employee of the Year
David Scott
Office of the Designated Approving Authority, Industrial Security Field Operations (ISFO) Directorate

2012 Team of the Year: Operations Analysis Group
Michael Buckley, *Chief, OAG, Counterintelligence (CI) Directorate*
Andrew Woods, *OAG, CI*
Tina Talley, *OAG, CI*
John Massey, *OAG, CI*
Michael Pietrowski, *ISFO*
Dianne Taft-Moore, *Industrial Security Policy and Programs Directorate*
Kimberly Jiles, *Personnel Security Management Office for Industry (PSMO-I)*
Jason Chaffin, *PSMO-I*
Alan Hern, *CI*
Joseph Conrey, *CI*
Patricia Burke, *CI*

2012 Employee of the 1st Quarter
Adam Hauch, *CI*

2012 Employee of the 2nd Quarter
Kimberly Jiles, *PSMO-I*

2012 Employee of the 3rd Quarter
Randy Staples, *Support Services Division*

2012 Employee of the 4th Quarter
Dustin Sievers, *Virginia Beach Field Office, ISFO*

VIP ADDRESSES SUPERVISORS

HAMRE ISSUES CHALLENGE TO EMBRACE NEW THINKING

DSS was honored to host Dr. John Hamre, president and chief executive officer of the Center for Strategic and International Studies (CSIS), for a presentation during the field supervisor's training event.

In his introductory remarks, Stan Sims, DSS Director, called Hamre a friend of DSS who is devoted to making the world a better place. Prior to joining CSIS, Hamre held a number of positions that provided a unique perspective on government operations. Hamre was the 26th Deputy Secretary of Defense, Under Secretary of Defense (Comptroller), and is currently Chairman of the Defense Policy Board. Before serving in the Department of Defense, Hamre worked as a professional staff member of the Senate Armed Services Committee and in the Congressional Budget Office.

In his remarks, Hamre challenged the audience to stop doing "dumb" things and adjust to a 21st century security environment with 21st century tools. "Don't do dumb things that mean we lose our capability to do good things," he said.

Hamre opened his remarks by saying he was at DSS to pay compensation from his time as Comptroller. "While I was Comptroller, I oversaw serious cuts to the DSS budget that really hurt DSS. I was wrong," he said. "It took me awhile to realize it, but by helping DSS, we are helping the country and our national security."

Since that time, Hamre said he has watched the transformation of the agency from one that was broken to one that was doing exciting things.

He added that he would like to see that spirit and those ideas drive a larger transformation of security operations in the Department.

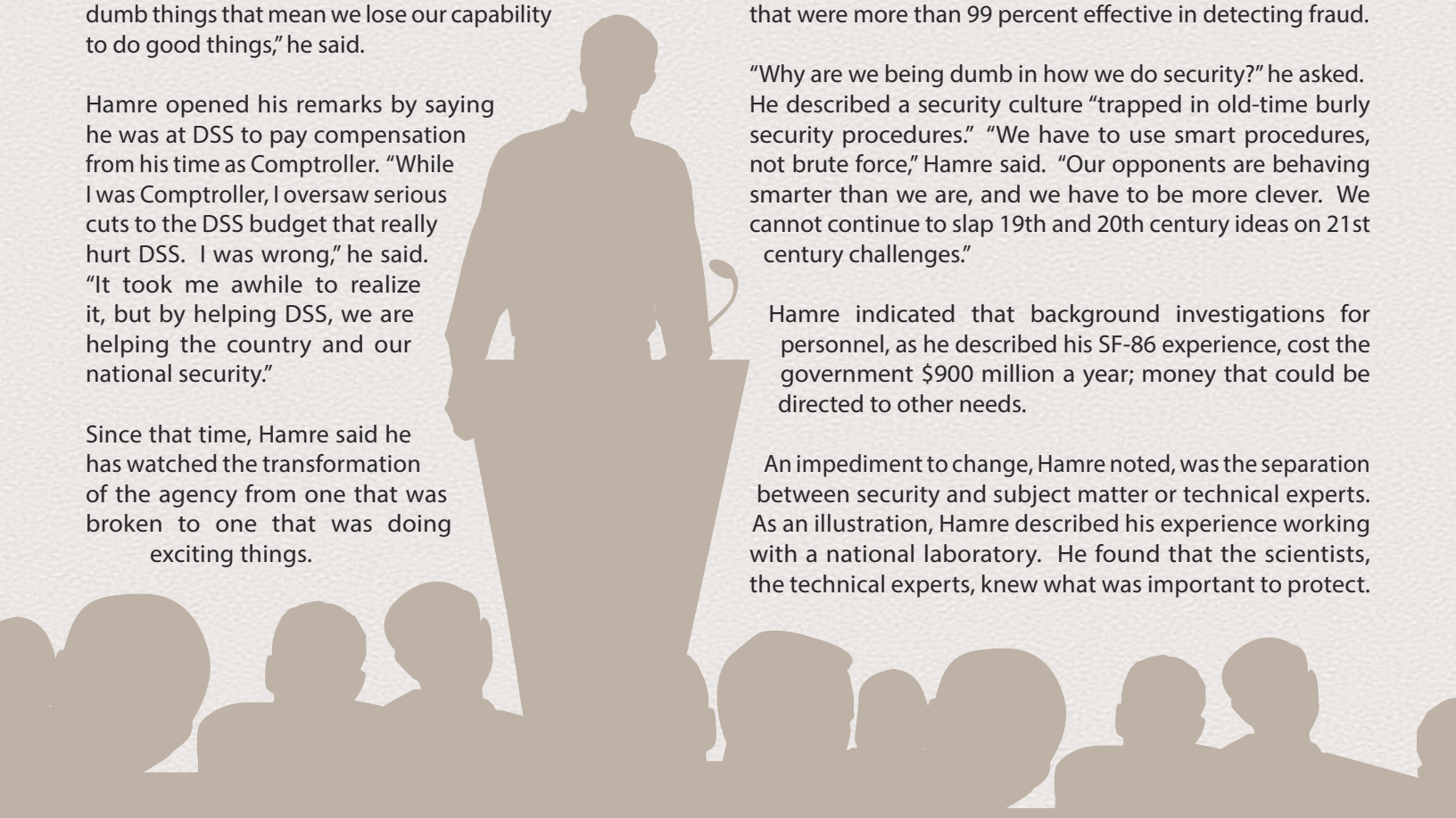
With a liberal dose of humor, Hamre recounted his experience in applying for his periodic reinvestigation as an example of a "dumb" process that needs to change. Hamre noted that he travels well over 100,000 miles per year and still holds a high level of personnel security clearance eligibility. His personnel security clearance application, though, asked him to document every instance of foreign travel and every foreign contact. He refused to provide the data and described the 90-minute interview with the investigator assigned to his case.

"We went over my response to every question on the SF-86," he said. "If I lied on the application, was I going to admit it to the investigator? Is this really the best way to catch a spy?" Hamre noted that he worked for a company that aggregated data and was able to develop a series of six simple questions that were more than 99 percent effective in detecting fraud.

"Why are we being dumb in how we do security?" he asked. He described a security culture "trapped in old-time burly security procedures." "We have to use smart procedures, not brute force," Hamre said. "Our opponents are behaving smarter than we are, and we have to be more clever. We cannot continue to slap 19th and 20th century ideas on 21st century challenges."

Hamre indicated that background investigations for personnel, as he described his SF-86 experience, cost the government $900 million a year; money that could be directed to other needs.

An impediment to change, Hamre noted, was the separation between security and subject matter or technical experts. As an illustration, Hamre described his experience working with a national laboratory. He found that the scientists, the technical experts, knew what was important to protect.



"USE YOUR BRAINS, NOT YOUR

WORDS OF WISDOM: Dr. John Hamre, President and Chief Executive Officer of the Center for Strategic and International Studies, provides the key note presentation during the field supervisor's training event. *Photo: Stuart Stahl*

While the security personnel were doing a number of activities, they didn't even know what the lab was working on. "There needs to be a fabric of trust and understanding," Hamre said. "It's the only way to find the anomalies."

Hamre lauded the DSS approach to partnership and building trust with industry. "Every company wants good security for their own self-interest," he said. "You need to help them get better. You need to be a worthy partner before people will trust you."

In closing, Hamre challenged the audience to "use your brains, not your fingers." "The DSS mission is bigger than you realize and more complex. The world is changing, and you have to change to be able to help industry be successful."

FINGERS"

LEADERSHIP CHALLENGES OF THE FUTURE

By Adriane D. Johns
Industrial Security Field Operations

"Leadership Challenges of the Future" was the theme for the annual Supervisor's Training Meeting, held by Industrial Security Field Operations (IO) in February at DSS headquarters in Quantico, Va. The training provided IO supervisors with pertinent policy updates, an overview of current strategic objectives, details of past successes upon which to build future goals, ongoing and new initiatives, and leadership development training.

The guest speaker for the event was Dr. John J. Hamre, president and chief executive officer of the Center for Strategic International Studies, Inc., a public policy research institution that provides strategic insights and bipartisan policy solutions to help decision makers chart a course toward a better world. (For a recap of Dr. Hamre's presentation, see the accompanying article.)

The training agenda also included an agency update and overview by DSS Director Stan Sims. Sims provided supervisors with his vision for the future and way forward for DSS in 2013. Afterwards, he answered questions from the group.

During the three days, DSS presenters provided updates and outlined new initiatives that will have a direct impact on field operations, and the scheduled implementation of these initiatives. The Quality Assurance office introduced several initiatives involving workload prioritization and the development of innovative products that support DSS personnel in executing the mission.

Other topics focused on cybersecurity, Electronic Control Plans for cleared companies operating under Foreign Ownership, Control or Influence, administrative inquiries, and the facility clearance process. The new Personnel Security Management Office for Industry (PSMO-I) provided an overview of the changes to the personnel security mission resulting from the consolidation of the military Central Adjudication Facilities and the Defense Industrial Security Clearance Office into the new Department of Defense Consolidated Adjudication Facility.

"The highlight of the week was certainly Dr. John J. Hamre's discussion; he challenged us to not only be innovators, but problem solvers," said Matt Roche, field office chief of Alexandria Field Office 1.

The attendees, comprised of field office chiefs, information system security professional team leads, personnel security branch chiefs, regional operations managers and regional directors, came from the four regional areas of operation and the newly established PSMO-I.

IO OBJECTIVES:

1. Improve capability to detect and mitigate security vulnerabilities.
2. Establish the Personnel Security Management Oversight for Industry mission.
3. Develop cyber capabilities to support emerging cyber requirements and policy.
4. Maintain and strengthen customer and stakeholder relationships.
5. Deploy technology solutions that increase efficiency and effectiveness.
6. Enhance infrastructure to improve organizational effectiveness.
7. Recruit, develop and retain personnel.
8. Develop and execute strategic communications plan.

FIELD OPS

IMPLEMENTS STRATEGIC OBJECTIVES

Winston Churchill said, "To improve is to change; to be perfect is to change often." To ensure it is able to quickly adapt and change to a dynamic mission and environment, Industrial Security Field Operations (IO) developed eight objectives for Fiscal Year 2013 with the plan of reviewing them annually to ensure their relevancy.

The objectives were developed during an IO senior leader off-site in November 2012, which included leaders from the four regions, Personnel Security Management Office for Industry (PSMO-I), and the IO headquarters staff.

"The IO Strategic Objectives provide the foundation for those priority initiatives and projects IO senior leaders feel are critical to our success in FY13 and beyond," said Richard Lawhorn, Director of IO. "IO objectives are closely aligned with the DSS Strategic Plan and reflect our emphasis on the workforce, continued process improvement and needed efficiencies in a time of budget constraints across the U.S. government."

In developing the objectives, the group considered a variety of information, to include the DSS Strategic Plan and the results of the DSS Climate Survey, and looked at possible updates to existing programs and processes. Each objective has a designated owner within IO, who serves as champion for the effort and engages with customers to gain acceptance of the objective's deliverables.

Objective 1 is an example of validating a process. It will analyze the security assessment process from beginning to end. The review will determine the relevancy of the process, whether any updates need to be made, and ensure the assessments are targeting the right vulnerabilities to mitigate risk. In order to gather experience from across the regions, this objective requires the establishment of a working group to determine the validity of the assessment process.

Objective 2 was developed in response to an identified need and calls for the creation of the PSMO-I. This objective was a direct result of the consolidation of the Department's Central Adjudication Facilities and the need for DSS to maintain its role as the liaison for industry. The PSMO-I will fill that role for DSS.

Objective 3, which focuses on developing cyber capabilities to support emerging cyber requirements and policy, was established in response to new developments in the DSS mission.

Objective 4, which focuses on development and deployment of technology solutions, is designed to ensure successful deployment of the Office of the Designated Approving Authority Business Management System in 2013. It also begins the requirements definition process for the National Industrial Security System, which will replace the Industrial Security Facilities Database in the future.

Objective 5 was established to help improve internal IO operations by creating a new office to centralize all IO administrative functions, and become the IO interface with other DSS offices. This office will oversee the processes for staffing, taskings, etc., and work to improve organizational effectiveness.

Objective 6 will address workforce concerns identified in the recent climate survey. This objective will focus on training the workforce through formal training but also through leadership and professional development. It will also look at promotion opportunities and the use of retention tools.

The IO objectives align with specific agency strategic goals, and results will be reported

WHAT IS AN ISL?

The Defense Security Service (DSS) Industrial Security Letters (ISLs) periodically clarify, interpret, or give guidance to cleared contractors on developments relating to industrial security. These documents are intended to assist cleared contractors carry out their responsibilities under the National Industrial Security Program and provide security-related implementation guidance.

DoD Directive 5220.22, National Industrial Security Program, provides the authority for DSS to issue an ISL. The ISL is a tool to ensure cleared contractors are provided up-to-date guidance on their implementation of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)."

An ISL does not, however, establish policy for the National Industrial Security Program.

When a NISPOM policy implementation issue is identified by DSS or a cleared contractor, a determination is made as to the overall impact. The first step is to determine if the specific policy issue and/or question is isolated to that facility or has far-reaching effects. If so, it may require clarification, interpretation, or additional guidance. If the issue is isolated, clarification of the policy requirements with the cleared contractor or a posting on the DSS website with a notice or frequently asked question may suffice.

Broader issues are best addressed in an ISL. Once DSS identifies the need for an ISL, the DSS Policy Division drafts and coordinates the ISL. After DSS Director approval, the ISL is sent to the Office of the Under Secretary of Defense for Intelligence who serves as the principal staff assistant for industrial security policy, which includes the NISPOM. The ISL is then coordinated with the Information Security Oversight Office and the other cognizance security agencies under the NISP, to include the Director of National Intelligence, Secretary of Energy, and the Nuclear Regulatory Commission.

This coordination ensures that the interpretation or guidance is within the bounds of the policy. After coordination and review by DoD General Counsel, the ISL is approved for release by the Under Secretary of Defense for Intelligence. DSS then promulgates the ISL to cleared industry.

Unlike many other guidance documents, ISLs do not expire. They are incorporated into the NISPOM when the issuance is revised, they may be rescinded, or in some cases, they are re-issued when the guidance is required to be retained as an ISL.

DSS welcomes suggestions for ISLs. Suggestions or questions about specific information in ISLs can be sent to Policy_HQ@dss.mil.

The most recent ISLs issued in 2013 include:

ISL 2013-01 *Facility Clearance (FCL) Eligibility Requirements (NISPOM 2-201)*

ISL 2013-02 *National Archives & Records Administration Agency Agreement (NISPOM 1-103.b.)*

ISL 2013-03 *Transfers of Defense Articles to Australia without License or Other Written Authorization*

From 2006 to present are available at:

www.dss.mil/isp/fac_clear/download_nispom.html.

back to the DSS Executive Steering Committee. For instance, IO Objective 5, "Deploy technology solutions that increase efficiency and effectiveness" is tied directly to DSS strategic goals 3 and 5. (Ensure DSS information technologies are responsive to DSS employees, customers, and stakeholders; and incorporate shared lessons in meeting agency goals).

Although IO developed the objectives for FY13, the plan is to update them annually. Each objective owner will revalidate the need and adjust accordingly, whether it means changing the focus of the objective, continuing on the same path, or deleting the objective altogether. While IO doesn't expect to be perfect, as Mr. Churchill's quote suggests, these objectives will help ensure it continues to improve.

"We look forward to an outstanding year, and as always, appreciate the great work done every day by our outstanding industrial security professionals in the field," Lawhorn said.

DSS COUNTERINTELLIGENCE CELEBRATES 20TH ANNIVERSARY

Twenty years ago, on February 25, 1993, the acting Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures, Ray Pollari, signed a letter that stood up a Counterintelligence (CI) Office in the then-Defense Investigative Service. The establishment of a separate CI office was a groundbreaking and trend-setting action.

In the mid-1970s, due to misuse of information concerning U.S. persons by the Department of Defense (DoD), the intelligence oversight response resulted in a separation of the CI aspects of DoD from general security functions and practices. Executive Order 12333, first approved in 1981, defined CI as "information gathered and activities conducted to protect against espionage, sabotage, or international terrorist activities, but not including personnel, physical, document, or communications security programs."

It wasn't until the 2009 iteration that Executive Order 12333 removed that exception from the definition of CI. So DoD's 1993 incorporation of a functional CI element in an agency that focused largely on the application of security missions and functions to U.S. persons was groundbreaking for its time.

The original DSS CI office of 1993 consisted of detailees from each of the armed services, led by Joseph Riccio, Naval Criminal Investigative Service agent, and supported by Julie Miller, office administrator and Laurie Dungan, a training professional from the DoD Security Institute..

Since the office's inception, each of its nine directors has left a positive mark on its evolution, growth, and recognition for contributions to national security. The efforts of DSS CI personnel have helped to mold the office's mission and have made possible its many successes:

- **Arrests of bad actors; continued growth in actionable leads;**
- **Publishing of thousands of Intelligence Information Reports;**
- **Increased industry reporting;**
- **Development and dissemination of hundreds of community- and industry-driven threat products; and**
- **Greatly expanded outreach programs to develop threat awareness in the cleared contractor community.**

With its dedicated workforce, the DSS CI Directorate will continue over the coming decades to provide even greater assistance to DoD, DSS, and cleared contractors in ensuring the nation's security.

SYMPOSIUM BRINGS TOGETHER ACQUISITION & SECURITY

DSS Director Stan Sims participated as a subject matter expert and panel member at the Intelligence and National Security Alliance (INSA) Security Policy Reform Council (SPRC) symposium held in March at SI Organization, Inc., Chantilly, Va.

More than 200 senior security and acquisition personnel from government and industry attended the symposium. The theme was "Next Steps in Security Reform: Overcoming Disconnects among Acquisitions, Security, and Industry."

The symposium, led by the Honorable Charles Allen, INSA senior intelligence advisor and SPRC chairman, highlighted current initiatives designed to remedy disconnects between acquisition and security and provided valuable insight into the effects of sequestration.

Delivering the keynote address was the Honorable Stephanie O'Sullivan, Principal Deputy Director of National Intelligence (DNI), who spoke about the significant accomplishments made in the security clearance process, specifically the reduced timelines and the need to build upon the gains made in the past several years. Her address emphasized the need to continue the progress made in standardizing security policies and bolstering partnerships between government and industry, as well as between INSA and the government workforce.

The day's first panel, "Acquisitions Strategies and Plans for Meeting Future Needs," featured acquisition executives from the Central Intelligence Agency (CIA), National Security Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office (NRO), Defense Intelligence Agency, DNI, and the Department of Defense. The purpose of the panel was to clarify how the acquisition community has adopted processes to respond to the deluge of requirements since the terrorist attacks of Sept. 11, 2001, and how those processes will change in the coming years as resources become more scarce.

As a participant in the symposium's second panel, Sims discussed "Security Challenges in Aligning Acquisitions Processes," along with Jamie Burnett, Director of Security, NRO, and Mary Rose McCaffrey, Director of Security, CIA. Sims spoke about the need for greater efficiencies and reforms in security and acquisitions to meet fiscal challenges while protecting our nation against a world of evolving threats, especially in the Defense Industrial Base.

The partnership between INSA and DSS is an example of working together for continued reform, and Sims recognized that "this partnership is representative of how the intelligence community should address the inconsistencies and disconnects between security and acquisitions." He also discussed the efforts DSS has made to bring these two communities together, and that he and Brett Lambert, Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy, have vowed to bridge the gap together.

The day's third panel, "Mechanisms for Addressing Disconnects between Acquisitions and Security," was designed to identify relevant and actionable reforms. Moderated by INSA SPRC Vice Chair Kathy Pherson, the panel discussed various pathways to bridge the gap between acquisitions and security. One suggestion was to scope the issue and create a team of procurement, acquisition, and security experts from government and industry to study a specific case, where the costs of current policy can be identified and measured.

Following the morning's panels, Sims led a lunch breakout session that allowed attendees and panelists an opportunity to share an unstructured, candid discussion on specific issues of interest. He emphasized the strong partnership DSS has cultivated with industry and government stakeholders in execution and oversight of the National Industrial Security Program. The final panel, "Looking to the Future," featured members of DNI, U.S. Army, and industry representatives to suggest ways that government and industry can utilize the most cutting edge technologies for security clearance applications.

>> ASK THE LEADERSHIP

A Q&A WITH **KEVIN JONES**, DIRECTOR,

"THE CHOICE IS TO **LEAD CHANGE** OR **SUFFER IT**."

Kevin Jones has been the Director, CDSE, since 2001. In this position, he is responsible for furnishing unparalleled development, delivery, and exchange of security knowledge to ensure a high-performing workforce capable of addressing our nation's security challenges.

Since joining DSS, Jones has served in a number of positions with increasing authority, to include working as a case analyst at the Personnel Investigations Center (PIC), staff officer in the PIC Operations Management Office, and DSS international projects officer. He was the Chief, PIC Operations Management Office and Chief of the PIC's Investigations Division. He also served as the Director, Operations Center – Baltimore, Deputy Chief of Staff for Personnel Security Investigations, and Personnel Security Investigations Program Manager.

Jones sat down with the ACCESS editorial staff to discuss changes in how CDSE delivers training and education and how he sees the new Innovation Office fitting into DSS operations.

When you became the Academy Director, most of the training was done in-house in classroom-style settings. In FY12, CDSE had 324,838 course completions. How has CDSE managed the transition from classroom-based to web-based training?

We haven't really transitioned away from the traditional instructor-led classroom training into a web-based training environment but rather have made significant strides towards a blended-learning approach. In many cases, these eLearning courses serve as prerequisites for students attending instructor-led courses, but they are also available for both security professionals and non-security practitioners to take advantage of anytime, anywhere.

Taking these eLearning courses as prerequisites facilitates achievement of foundational knowledge by the students before they enter an instructor-led course and provides for more classroom time to be dedicated to the application of knowledge and skills through practical exercises and simulations. In addition, this blended learning approach reduces the amount of time students are away from their respective commands or organizations and is often a significant savings of scarce TDY funds.

The blended approach also includes the use of performance support tools such as job aids, videos and "shorts" that are easily accessible via the CDSE website. Accessing information when it is needed (on demand) is a critical element in supporting the DoD security enterprise and industry under the National Industrial Security Program (NISP).

One of CDSE's newest efforts is security webinars. We are providing timely 30-minute weekly webinars on a variety of security hot topics for industry and DoD that can be accessed real time or at a later date in the webinar archive.

How has the role of the instructor changed in this new environment?

The role of the instructor has evolved along with CDSE's products and services. Today's CDSE instructors serve not only to teach courses but also serve as subject matter experts. In this capacity they play a critical role in the development and maintenance of courses and performance support tools. They also provide information support to the security community through advisory and consulting services provided to our DoD and industry customer bases.

With the addition of CDSE's Education Program, we have more than 15 subject-matter experts (SME) under contract to instruct the advanced education courses. These SMEs have advanced degrees and specialized experience, as well as experience teaching at the collegiate level. These expert adjunct instructors give CDSE the ability to include world-class SMEs as part of our team to deliver graduate-level courses.

DoD Instruction 3305.13, assigned the DSS Director as the functional manager for security training within the Department of Defense. How did this instruction change or affect how CDSE approached its mission?

This instruction served as the driving force behind the institution of the CDSE. Specifically, the instruction formally directed DSS to deliver security training across the primary security disciplines and specialty areas. Using instructional design and development principles called out in the instruction, CDSE built its security education and training curricula centered around the community and defined DoD Security Skill Standards.

Further, the instruction also required DSS to establish the DoD Security Training Council (DSTC). In addition to its advisory role, the DSTC has been instrumental in the development of the SPēD Certification Program and serves as the governance board for SPēD's core certifications. Through these efforts, the CDSE has worked closely with the security community and has developed a collaborative approach to the development and delivery of security education, training, and professionalization products and services.

The Security Professional Education Development (SPēD) Program has been a significant focus and achievement for CDSE and DSS. What is next for the program?

The next step for the SPēD program is to not only complete the development of the certification portion of the program but to complete the implementation of SPēD as a holistic approach toward workforce professionalization that includes education, training, and certification.

The SPēD Certification Program has been in continual development since its inception in 2009. Current challenges require the CDSE to address the development of multiple certifications, achieve accreditation for each certification from the National Commission for Certifying Agencies (NCCA), deliver testing venues (to promote the "anytime, anywhere" approach), and provide career support tools delivered at the right time in the right quantity for the right individuals who are charged to meet our nation's security challenges.

These challenges cannot be addressed solely by DSS. What I mean by this is that the success of the certifications thus far is the fact they've been built by the community for the community. From the development of the DoD Security Skills Standards, to the content of certification test questions, and even voting on the cut scores for certification exams, it is all done with community representation through the DoD Security Training Council.

Although we are realizing great success with the national accreditation of the Security Fundamentals Professional Certification by NCCA and the initiation of commercial testing, we know programmatically we are still in the development stages. I can foresee over the next two years, we'll move to having all four core SPēD certifications and four specialty certifications into the maintenance and sustainment phase.

Additionally, full integration of security education and training as part of the SPēD program is critical to the professionalization of the DoD security workforce. This involves validation of courses against the DoD Security Skill Standards, development of career maps for security professionals, and initiation of the certification maintenance program designed to promote career growth while supporting DoD security needs of today and tomorrow.

Can students earn college credit by completing CDSE courses?

The short answer is yes. Several CDSE courses now carry college credit equivalency recommendations. The American Council on Education's College Credit Recommendation Service (ACE CREDIT) has evaluated and recommended college credit for 13 of CDSE's courses.

CDSE is currently working with ACE CREDIT to review several more courses for credit recommendations. This enables students who complete designated CDSE courses the opportunity to request college credit for CDSE courses and apply them to colleges and universities toward degree or certificate programs.

More information on how to request college credit is available at the ACE CREDIT website at www.acenet.edu/credit.

DSS recently established an Office of Innovation under your leadership. What are your goals for this new office? And why must DSS "innovate?"

The goals for this new office, when it is fully operational, are to lead and/or facilitate change in DSS. Using a well-defined innovation process, the office will transform ideas from people into practices or technology that improve the effectiveness and efficiency in the ways we conduct the DSS mission and support. In the near term, the office is acquiring staff and infrastructure to support an initial operational capability by the end of FY13.

DSS recognizes that innovation is a strategic necessity. Evidence overwhelmingly demonstrates that organizations that do not innovate operate at greater risk. The choice is to lead change or suffer it.

SPēD CERTIFICATION TESTING NOW AVAILABLE WORLDWIDE

In February 2013, the Center for Development of Security Excellence (CDSE) began offering the Security Fundamentals Professional Certification (SFPC) and Security Asset Protection Professional Certification (SAPPC) at commercial testing centers worldwide.

Through a contract with Pearson VUE, opportunities for Department of Defense (DoD) security professionals and practitioners to take Security Professional Education Development (SPēD) certification assessments became significantly more convenient. The commercial testing contract provides access to over 1,000 testing centers worldwide, 250 of which are on DoD installations.

"This is an exciting capability for the certification initiative," said Kevin Jones, Director of the CDSE. "The partnership with Pearson VUE and commercial testing expands the accessibility of testing opportunities available to all security professionals and practitioners worldwide."

The SPēD Certification Program, administered by the CDSE, is intended to ensure there is a common set of competencies among security practitioners promoting interoperability, facilitating professional development and training, and developing a workforce of certified security professionals. CDSE is closer to achieving that goal with the availability of commercial testing.

To learn more, please visit http://www.cdse.edu/index.html.

BETA TESTING CONCLUDES FOR SECURITY PROGRAM INTEGRATION PROFESSIONAL CERTIFICATION (SPIPC)

From November 2012 to January 2013, the Center for Development of Security Excellence (CDSE) conducted beta testing of the Security Program Integration Professional Certification (SPIPC). SPIPC is the third level of the Security Professional Education Development (SPēD) Program.

In total, 174 security professionals participated in the SPIPC beta assessment, ensuring DSS had the beta test results required to move SPIPC to the next level of certification development.

The topic areas of the SPIPC assessment differ from the Security Fundamentals Professional Certification (SFPC) and Security Asset Protection Professional Certification (SAPPC) — the first two levels of the program — as the topics include security program management and risk management. Although SPIPC beta participants were required to have both SFPC and SAPPC, the production release will only require SFPC certification for SPIPC candidates.

The DoD Security Training Council reviewed results from the beta test to develop the production version of SPIPC and determine the passing score. Of the beta testers, 99 names were forwarded to the Undersecretary of Defense for Intelligence for conferral.

The SPIPC assessment test was made available to all SPēD conferees that are eligible through CDSE's commercial testing partner, Pearson VUE, in April 2013. Resources for the SPIPC, including the SPIPC preparation tools, are available on the CDSE website.

CDSE TRAINS AFGHAN MILITARY IN POLAND

The Center for Development of Security Excellence (CDSE) delivered personnel security investigation and adjudication process training at the NATO Joint Forces Training Center, Bydgoszcz, Poland, in March 2013.

The Afghan government requested training geared toward refining their personnel security processes and techniques for clearing and vetting Afghan nationals as part of their efforts to build a stable government structure. DSS received the request from the NATO Training Mission-Afghanistan (NTM-A) commander to provide training to 15 military officers from the Afghanistan Ministry of Interior Affairs and Ministry of Defense. The training, held in support of NTM-A, was the culmination of a long coordination process that began in August 2012.

"It was amazing to watch the transformation of the Afghan students throughout the course as they eagerly received the training we provided," said Walter Hayward, CDSE Personnel Security instructor. "While they still have some obstacles to overcome, we have hopefully given them the knowledge and tools to help them move forward with their security programs and processes."

Teaching in the NATO facility and in Poland required the instructors to be flexible and innovative. By using the same course materials instructors used for training in Iraq in 2011, and applying lessons learned from their Iraq experience, the instructors refined the investigative and adjudicative perspective to allow the Afghans to use and apply the U.S. process.

Five interpreters were provided to help translate instructional material to Dari, the Afghan language. After discussing several slides, the instructors realized that the interpreters required several examples for translation because many English words had no direct translation to Dari. Although course materials were translated before the instructors' arrival, further interpretation was often needed throughout the course.

Despite being challenged with cultural, legal, and language differences, the instructors were able to deliver their instruction effectively, as all 15 students successfully completed the training. The NTM-A voiced a clear interest in continuing relations with CDSE and requested this same course be provided to another group of students in the near future.

BREACH EXPOSES DANGER

In January 2012, the information technology (IT) department of a cleared company detected activity on their unclassified network which was traced to a "key logger/thumb drive" attached to a desktop computer.

The cleared company uses a host-based security system that detected the presence of the thumb drive almost as soon as it was connected to the network. The facility security officer (FSO) reported the incident to the Defense Security Service the same day it was discovered. The information was also locally referred to two federal investigative agencies.

The computer was assigned to an engineer with a Secret personnel security clearance (PCL) and NATO briefing. The engineer worked on a program that is part of a classified contract with the U.S. Navy and fell under International Traffic in Arms Regulations (ITAR) guidelines. The engineer did not have access to the cleared laboratory facilities or to Department of Defense-accredited IT systems.

Federal investigative agencies visited the company immediately, where they were met with some initial resistance. The company considered the situation to be a breach of company policy rather than a counterintelligence (CI) issue or a potential criminal act.

In February 2012, DSS representatives met with the company's FSO, legal counsel, and president to discuss the incident further. The legal counsel and president were of the opinion that this was an internal matter that could be resolved by terminating the employee. The DSS representatives reminded the company that keylogging software can be used to acquire system passwords and transmit data; therefore, further evaluation of the thumb drive would be beneficial in resolving any potential concerns.

The company reviewed the thumb drive and stated they found nothing nefarious on it. However, they did admit it contained keylogging software.

A keylogger *is a hardware device or a software program that records the real time activity of a computer user, including the keyboard keys they press. Keyloggers are often used in IT organizations to troubleshoot technical problems with computers and business networks. Keyloggers can also be used to monitor network usage of people without their direct knowledge. Finally, malicious individuals may use keyloggers to steal passwords or other sensitive information.*

Keylogger software *is freely available on the Internet. They allow not only keyboard keystrokes to be captured but also are often capable of collecting screen captures from the*

OF KEYLOGGER SOFTWARE

computer. Normal keylogging programs store their data on the local hard drive or an attached device, but some are programmed to automatically transmit data over the network to a remote computer.

After completing the review, the company turned the thumb drive over to a federal investigative agency, which opened a full field investigation.

The company asserted the thumb drive belonged to the engineer on whose computer it was found and that he placed it there. The engineer however, stated the thumb drive was not his and claimed he did not know it was attached to his computer. During the course of the investigation, a removable hard drive was found in the engineer's work area, which was subsequently found to contain pornographic images. The engineer admitted to owning the hard drive. The company also discovered the engineer had pictures on his cell phone of unclassified areas of the facility as well as pictures of other employees, which were taken without their knowledge.

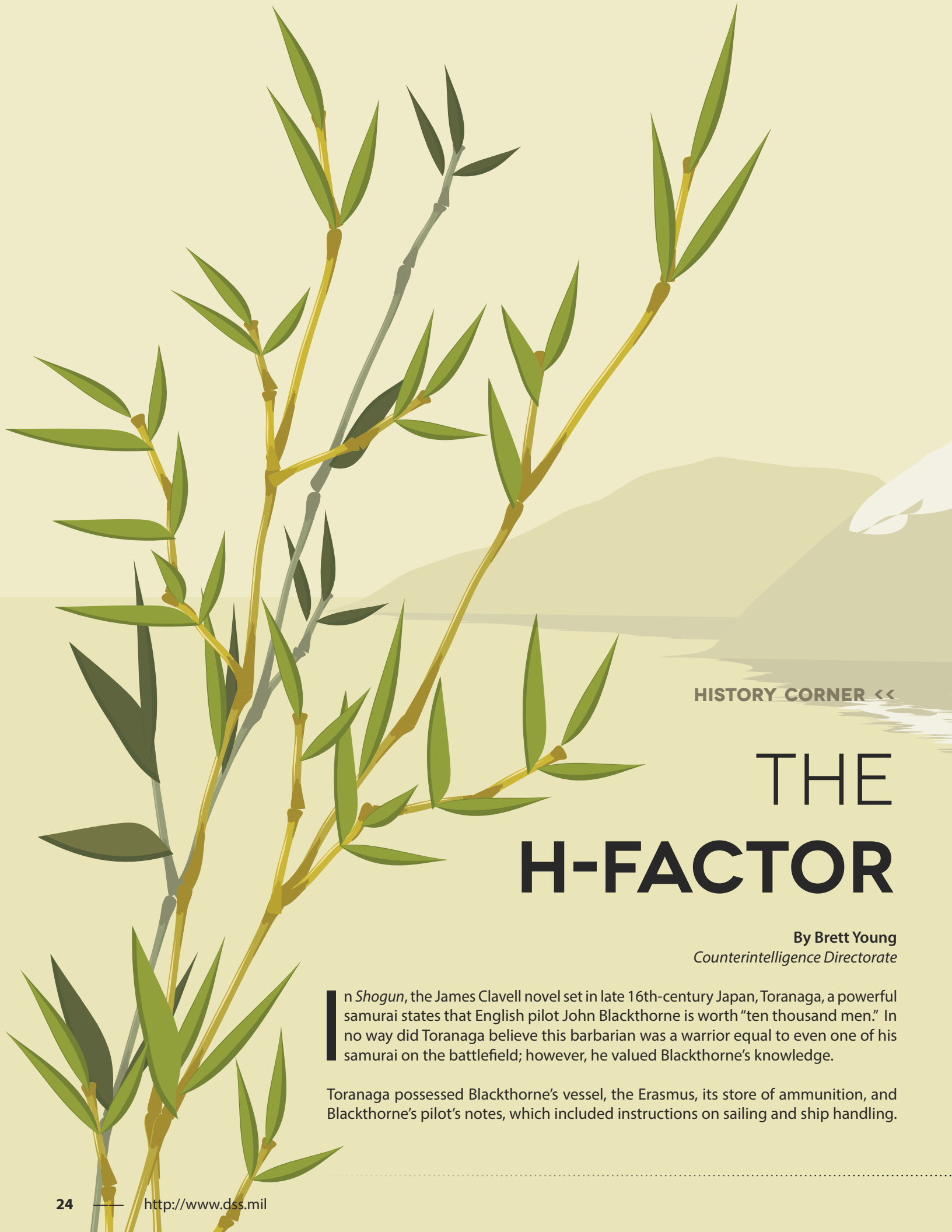
Based on this information, the engineer resigned in lieu of being terminated for not following company policy regarding use of removable media on the company's network and for taking pictures of unclassified areas of the facility, not for reasons related to PCL eligibility. The company updated the Joint Personnel Adjudication System, annotating the engineer's separation and submitted an incident report. The then-Defense Industrial Security Clearance Office entered a Loss of Jurisdiction.

WHAT WE LEARNED:

The company should be complimented on its effective audit and monitoring of its information systems. The software was able to immediately identify and locate the thumb drive breach, which effectively shut down the potential download of information. The company also included the download restrictions and penalties in its security program policy, which allowed the termination of employment.

The company, DSS, and the federal investigative agencies were able to quickly move past the initial resistance by determining the incident did require a deeper look through a "CI and security" lens.

This incident emphasizes the value of open and solid lines of communication between DSS and industry, as well as the importance of counterintelligence awareness training provided by the DSS Center for Development of Security Excellence.



THE H-FACTOR

By Brett Young
Counterintelligence Directorate

In *Shogun*, the James Clavell novel set in late 16th-century Japan, Toranaga, a powerful samurai states that English pilot John Blackthorne is worth "ten thousand men." In no way did Toranaga believe this barbarian was a warrior equal to even one of his samurai on the battlefield; however, he valued Blackthorne's knowledge.

Toranaga possessed Blackthorne's vessel, the Erasmus, its store of ammunition, and Blackthorne's pilot's notes, which included instructions on sailing and ship handling.

Toranaga realized that controlling the sea approaches to Japan would make him the most powerful lord.

However, Toranaga and his army lacked the knowledge to build more vessels or use them effectively to control the sea. Toranaga realized the value of Blackthorne's technical expertise: he recognized the human factor — or "H-factor" — required to apply new technology in the coming conflict with his rival lord, Ishido.

Benefiting fully from technology, whether acquired via legitimate or illicit methods, requires the knowledge to effectively apply the technology. The technical expertise necessary to accomplish the research and development (R&D), testing, manufacture, and application of novel technologies is not gained simply by stealing technical data, reverse-engineering illicitly acquired copies of the technology, or manufacturing duplicates.

This technical know-how resides in subject matter experts (SMEs). Thus, even in today's environment — characterized by daily reports of cyber intrusions and the use of complex networks of procurement agents — those collecting against U.S. technologies will continue to employ traditional intelligence methods to target SMEs within cleared industry.

Security and counterintelligence professionals protecting critical program and classified information must be vigilant regarding the continued threat of conventional human intelligence (HUMINT) in collection efforts.

In Clavell's novel, Toranaga believed a showdown with Ishido was imminent, so he did not have the luxury of investing time in shipbuilding and weapons research. His chosen shortcut to exploitation of the Erasmus and her cargo was the veteran pilot John Blackthorne.

Foreign collectors of U.S. technologies also seek shortcuts to avoid investing the time and resources required to research, develop, and exploit new technologies. Today's foreign collectors of U.S. technology leverage several methods to target SMEs working in cleared industry and academia.

In traditional HUMINT, collectors practice elicitation to extract preliminary information from a possible target for recruitment. The Defense Security Service Elicitation and Recruitment brochure describes elicitation as the art of conversation honed by intelligence services to its finest edge. It seeks to determine the target's access to the desired information, his or her susceptibility to recruitment, and the best approach to accomplish it.

Elicitation is often very subtle, consisting of seemingly meaningless small talk, so it can be hard to recognize. A relatively new elicitation technique exploits social networking sites to identify possible recruits and glean professional and private information about them so as to tailor an approach.

Following elicitation, a collector may attempt to recruit the target. An SME who becomes an "asset" not only provides access to much sought after data but can also aid in applying the stolen technology successfully.

During one conversation, Toranaga asked whether Blackthorne could build more ships like the Erasmus. Blackthorne stated he could if he traveled to England, recruited a cadre of shipbuilders, master seamen, and gunners, and then returned to Japan with several vessels to build Toranaga's fleet and train his crews.

Such a technology exchange would allow Toranaga to develop his own cadre of technicians to build and employ modern weapons, and ultimately, would allow Toranaga to control the seas around Japan.

Building a domestic cadre of SMEs can be difficult and costly, especially for countries subject to export restrictions, which limit access to new technologies. Countries developing their domestic R&D capability often employ academic solicitation to leverage their interactions with SMEs in the United States.

Intelligence collection via academic solicitation comes in several varieties. One method is to have students apply for internships with research programs dealing with the targeted technology. The students gain access to the data, then return home with improved skills to contribute to the R&D of new technologies.

Another form of academic solicitation consists of seemingly innocent requests for a SME to review an academic work. Typically, the researcher provides the SME with a draft paper, hoping the SME's feedback will help the researcher avoid spending time and money on dead ends.

Ultimately, in *Shogun*, Toranaga decided that the value of the SME, Blackthorne, was greater than that of the actual piece of technology, the Erasmus — so Toranaga covertly destroyed the vessel to prevent Blackthorne's departure from Japan.

Over 400 years later, even in the cyber era, the H-Factor — knowledge and skill resident in technical experts, researchers, and academics — remains as valuable as it was in sixteenth-century Japan. The skills, knowledge, and experience held by human beings remain vital to the research, development, and application of technology.

As long as it does, SMEs in cleared industry and academia will remain prized targets in foreign collection attempts against U.S. technologies.

“I HAVE BEEN BLESSED WITH THE MOST REWARDING MILITARY AND CIVILIAN CAREERS”

CUNNINGHAM
RETIRES FROM MILITARY

Larry A. Cunningham, Center for Development of Security Excellence (CDSE), retired from military service on Feb. 1, 2013, after serving more than 31 years in the United States Navy, both on active duty and in the Navy Reserve.

Cunningham, who serves as a Communication and Outreach specialist at CDSE, retired at the rank of commander as an information dominance warfare officer. He is a Vietnam era veteran, having served as an Air Force enlisted security policeman from 1971 to 1974. In 1984, he received a direct commission into the Navy Reserve as an intelligence officer, assigned to Reserve Intelligence Area, Washington, D.C.

His assignments include consolidated security manager and adjudicator assigned to Naval Intelligence Command; watch officer with Commander Naval Operations-Operational Intelligence/Pentagon; security manager and department head with Office of Naval Intelligence (two assignments); and his last assignment was at Defense Intelligence Agency (DIA), with assignment to the Joint Chiefs of Staff, Pentagon.

In 1994, he was assigned to Naval Investigative Service (NIS), now the Naval Criminal Investigative Service (NCIS). He attended the Reserve Basic NIS Agent course at the Federal Law Enforcement Training Center and was awarded the NIS Reserve Agent badge and credentials. He holds the distinction as being one of the longest serving Reserve agents assigned to NCIS.

"My most rewarding assignment as an intelligence officer was the 16 years I served as a Reserve agent for NCIS, formerly Naval Investigative Service," Cunningham said. "As a former agent for Defense Investigative Service, I was extremely proud to carry both credentials ... not many hold this distinction."

Immediately after the Sept. 11, 2001, terrorist attacks, he was mobilized to active duty with NCIS in support of Operations Noble Eagle and Enduring Freedom. He was assigned to the NCIS Protective Operations Directorate as a counterintelligence agent, with assignments throughout the United States, Europe, and Middle East area of operations (AOR).

During this time, he was instrumental in designing and co-instructing the first Reserve NCIS Agent course, during which Reserve intelligence officers assigned to NCIS received instruction in investigative interviewing, conducting port vulnerability assessments, intelligence collection methods and operations, report writing, and surveillance/counter-surveillance methods and techniques.

This course resulted in 29 intelligence officers being assigned to NCIS Reserve units nationwide, and receiving Reserve NCIS Agent status, with immediate deployment thereafter to worldwide assignments. Following his release from active duty in January 2003, he returned to work at DSS, but not for long.

"Following my release from active duty for Enduring Freedom/Noble Eagle in 2002, I was honored to be a by-name-request for recall to active duty with NCIS in support of Operation Iraqi Freedom," Cunningham said. "As an anti-terrorism/force protection officer, I travelled throughout the Middle East AOR in support of the NCIS mission and operations."

Since 2007, he supported the DIA, Joint Military Attaché School through participation in 17 joint military exercises to train U.S. defense attaches. His participation in the capstone exercise of a 13-week training program assisted in preparing nearly 900 defense attaches for post assignments in embassies worldwide.

"I have been blessed with the most rewarding military and civilian careers," Cunningham said. "I was privileged to serve my country as a member of the Armed Forces for 31 1/2 years. Now that I'm a few months away from retiring from DSS, I'm also bringing to an end 38 years with one agency, DSS — another honor!"

CAPITAL REGION CI ENHANCES

STRATEGIC PARTNERSHIP TASK FORCE A PAYOFF FOR

For a DSS field counterintelligence specialist (FCIS), it's all about "liaison," whether it's with the Industrial Security Representatives they support; with industry; or with their counterparts in the intelligence and law enforcement communities.

It is through this liaison that the FCIS cadre is able to collect information relating to illicit attempts to acquire U.S. information/technology and insider threats resident at cleared facilities, and refer that information to agencies in a position to act on it. Since fiscal year 2009, other U.S. government agencies have opened a significant number of investigations as a result of DSS Counterintelligence referrals; with the FBI accounting for approximately 50 percent of those open investigations.

To build on this relationship, the Capital Region CI team worked to develop better and closer liaison with the local FBI office, which led to the creation of a Strategic Partnership Task Force at the FBI's Washington Field Office in early 2012. The Strategic Partnership Task Force was established to include CI outreach to industry, and create opportunities for the two entities to work together in countering the threat to cleared industry through information sharing and joint support efforts.

After some discussion between the two offices, it was agreed that each Capital Region FCIS would undertake a four month rotation at the Washington Field Office beginning in June 2012. The FCIS spends at least one day a week with the Task Force, which has facilitated the relationship with squads and activities across the Field Office. The FCIS also supports the FBI on issues relevant to DoD and other Federal agencies performing work under the auspices of the National Industrial Security Program (NISP).

DSS CI participants are able to forge close working relationships with CI representatives from other U.S. government agencies assigned to the Strategic Partnership Task Force.

This working relationship has supported the outreach goals, as the both DSS and the FBI have conducted multiple joint briefings for cleared contractors. Not only do the two agencies benefit, industry benefits as well through fewer instances of duplicative outreach and better, more focused threat information. After a recent DSS/FBI joint threat awareness briefing, DSS received a letter from the President and Chief

LIAISON WITH FBI

ORGANIZATIONS INVOLVED

Executive Officer of a local cleared company stating, "…I appreciate your coordination and efforts to bring an FBI Special Agent to our training session — it is particularly refreshing to see the DoD and FBI working so closely together in this critical arena."

"The benefits of allowing your employee to have joint service experience are invaluable to the growth of both the FCIS in the assignment but also to for the awareness and understanding of capabilities of another intelligence community member," said Michael Clapp, chief of Counterintelligence Field Operations, Capital Region. "The relationship has allowed a more open, symbiotic flow of information benefitting the missions of both DSS and the FBI.

"Analytical collaboration occurs more frequently between our field CI analysts and analysts assigned to the Washington Field Office and it promotes information sharing under Executive Order 12333," Clapp continued. "This enhanced relationship has allowed for real time reactions to incidents occurring in the cleared contractor community which ultimately means more unified CI support for cleared contractors."

FCIS'S WORK MAY INVOLVE, BUT IS NOT LIMITED TO:

- Conducting CI collection and reporting in accordance with DoD Directives and NISP requirements;
- Perform CI awareness training for the cleared contractor population and/or individual training for high-risk personnel;
- Provide personnel security clearance status and history for persons of interest;
- Provide historical information on suspicious contact reporting, to include foreign targeting linked to specific cleared contractors, technologies, and personnel;
- Provide information on upcoming security vulnerability assessments at cleared facilities to allow for advance planning and coordination;
- Assist in introductions to cleared contractor personnel;
- Facilitate action on DSS referrals;
- Assist with events such as the FBI's Regional CI Working Group.

MARYLAND FIELD OFFICE ENCOURAGES DIVERSITY

To ensure employees have the opportunity to participate in and to expose them to a variety of diversity programs, the Maryland Field Office initiated "Diversity Days," with the first event held in February in recognition of Black History Month.

"The intent is to offer our employees the opportunity to recognize these celebrations, as not everyone is able to take part in the festivities offered at the Russell-Knox Building (RKB)," said Pamela Hunter, chief, Maryland Field Office. "We plan to continue this effort throughout the year in unison with those events offered at RKB."

The one-hour voluntary lunchtime sessions offer informal presentations, reading material such as pamphlets and books, and videos recognizing the various celebrations.

In February, Frank Husker, Senior Industrial Security Representative in the Maryland Field Office, gave a detailed presentation on Black History and slavery, oversaw a trivia game, and provided handouts about prominent Black Americans for attendees.

During the lunchtime event, attendees could watch video clips of Dr. Martin Luther King Jr.'s, "I Have a Dream" speech or one on the Tuskegee Airmen. Three other participants provided "Who Am I" skits, where they read a person's biography and the audience had to guess which famous individual they were portraying. Approximately 25 people from the Maryland field offices attended the event.

"I found the session held by Mr. Husker to be informative and enriching," said Brandon Pumphrey, Industrial Security Representative. "I have an enhanced appreciation of the session as the grandson of a World War II veteran and a native Marylander. As a DoD employee, I stand on the shoulders of the contributions that African-Americans made in the history of our Armed Forces, and the state of Maryland is robust with African-Americans who have made an everlasting impact on the history of the United States of America."

In March, the Maryland Field Office held an event at the Center for Development of Security Excellence in Linthicum, Md., to honor women in American history. The presentation focused on prominent women in the history of America, to include women pilots and women who worked on classified projects during World War II.

In a nod to the local area, it also recognized women from the National Security Agency (NSA) for their work in cryptology as well as women in Maryland who have made notable achievements in defense industry and women who have served in the military.

The presentation included material (information, photos, biographical data, and timelines) from NSA, the Johns Hopkins Applied Physics Laboratory, Northrop Grumman, the Department of Defense and featured historical video clips. The attendees participated in a word game to see who recognized names of important women in America's history, and prizes were awarded to attendees who completed a puzzle about women's history.

Depending on the level of interest and participation, the office is planning to hold events in May (Asian/Pacific American Heritage Month), September-October (recognizing Hispanic Heritage in America), and November (American Indian Heritage Month).

SAN ANTONIO FIELD OFFICE PRESENTS "DAY WITH DSS"

By Dawn Martin
Senior Industrial Security Specialist

On March 19, 2013, the Industrial Security Specialists of the San Antonio Field Office provided training across a wide range of topics essential to security professionals during a "Day with DSS."

Hosted by the NCMS Alamo Chapter, approximately 75 industrial security professionals attended the day of training, coming from as far away as El Paso (an eight-hour drive from the field office).

"I really enjoyed participating in our 'Day with DSS' event," said Industrial Security Representative Donna Heard. "It was an excellent opportunity to promote our relationships in a positive way with other security professionals and to take away ideas that can be used to enhance our presentations in future events."

IF THE EVENT HAD TO BE DESCRIBED IN ONE WORD, I WOULD CHOOSE 'DYNAMIC'

Robert Winslett, NCMS Alamo Chapter Newsletter Committee Chair, said it best, "Participation in a 'Day with DSS' was an event even for a seasoned professional to attend. As we listened closely to each of the team members and the material they thoroughly covered, one couldn't help but think about how their expertise and guidance has enabled facility security officers (FSOs) to succeed in the security arena.

"The training gave FSOs not only updated information, but each block of training allowed participants to ask those tough questions and receive detailed answers you don't see spelled out in the NISPOM [National Industrial Security Program Operating Manual]," Winslett continued. "We won't even mention all the networking! If the event had to be described in one word, I would choose 'dynamic.'"

The event was such a success that a second event is scheduled for May 14, 2013, and FSOs have asked if similar events could be held quarterly.

DEFENSE SECURITY SERVICE